Navy Marine Corps Intranet (NMCI) Legacy Applications Transition Guide (LATG) (Rapid Certification Phase)

Version 5.0

15 FEB 03

Prepared by:

NMCI Program Management Office – Technical Execution Division, PMW 164-4
Space and Naval Warfare Systems Command
Participants in the creation of this guide include:
Department of the Navy, Chief Information Officer
Program Executive Office – Information Technology
Information Strike Force
Customer Representatives from the Application Enterprise Action Group

Prepared for:

All NMCI Customers

THE NMCI LEGACY APPLICATIONS TRANSITION GUIDE IS PUBLISHED FOR INFORMATIONAL PURPOSES ONLY TO ILLUSTRATE LEGACY APPLICATIONS PROCESSES AND INTERACTIONS. THE CONTENT OF THIS DOCUMENT SHALL NOT BE CONSIDERED CONTRACTUALLY BINDING. ALL ISSUES ASSOCIATED WITH THE NMCI CONTRACT N00024-00-D-6000 SHALL BE REFERRED TO THE PROCURING CONTRACTING OFFICER, AT 703-685-5508

Disclaimer: This guide is intended for the customer. ISF procedures / processes are not fully detailed within this guide.

Record of Document Changes

Change No. and Date of Change	Date of Entry	Page Count Verified by (Signature)
1.0	14 March 2001	
1.1	18 April 2001	
2.0	13 July 2001	
2.1	26 October 2001	
3.0	19 April 2002	
4.0	30 June 2002	
4.1	15 August 2002	
5.0	15 February 2003	

For questions or suggestions to improve this guide please contact:

Space and Naval Warfare Systems Command (SPAWAR) Navy Marine Corps Intranet (NMCI) Program Management Office (PMO) San Diego, California

PMW 164-4, Technical Execution Division, Legacy Applications
619-524-7435

Information Strike Force
619-817-3856

TABLE OF CONTENTS

LIST OF FIGURES

Page

LIST OF TABLES

Page

1.0 CHIEF OF NAVAL OPERATIONS (CNO)

This document presents a complete baseline overview of the Legacy Applications Rapid Certification Phase of the Legacy Applications Transition Process. It is for Navy Marine Corps Intranet (NMCI) customers involved with transition activities. Information Strike Force (ISF) and Government program management personnel worked in close cooperation to design the processes, procedures, and policies described herein.

Naval message of 25 Feb 02 released by CNO N09T (date-time-group 252250Z FEB02) mandated Certification Phase transition guidance for NMCI. Director NMCI released a coordinated Naval message COMSPAWARSYSCOM/PMW164 242225Z MAY 02 with the Navy and Marine Corps Program Offices, and the NMCI ISF. This message further refined the transition processes in order to improve and accelerate near term NMCI seat rollout. The new process has been titled the "Rapid Certification Phase." This Transition Guide reflects the process and procedure changes outlined in these pertinent messages. The Chief of Naval Operations (CNO) assigned specific responsibilities to Echelon II Commanders in regards to identification, rationalization, submission, and accreditation of applications. These messages also described the division of NMCI Legacy Applications Transition into two distinct phases:

1. Rapid Certification Phase (covered in this guide)
2. Risk Mitigation Phase (addressed separately)

Additionally, the message focused on three keys to success as customers begin work on NMCI transition:

1. Site and Echelon II use of the ISF Tools Database (described here)
2. Reduction in the number of applications (guidance provided here)
3. Removal of certain accreditation requirements prior to seat Cutover to the Risk Mitigation Phase (guidance described elsewhere)

What is a Legacy Application?

The NMCI contract states, " An existing customer software application that is not included in the NMCI standard seat services or the CLIN 0023 catalog." It is an application in use today by persons performing missions or business for the Department of the Navy (DON). Legacy applications are *not* elements of the standard set services (also known as the Gold Disk), including those applications, which are available as a service via Contract Line Item Number (CLIN) 23.

Why Transition Legacy Applications to NMCI?

First and foremost, we are transitioning applications to NMCI, because NMCI is the new information technology (IT) environment for the Navy and Marine Corps. Second and subsequently, transition will enhance security, improve standardization, reduce

duplication/redundancy, and minimize software support costs. With this in mind, customers should make every effort to eliminate unnecessary, redundant, and nonstandard applications. They should do this in concert with their Echelon II Commanders.

Classified Legacy Application Transition Process

Transition processes for classified applications are similar to the steps and procedures for unclassified application, with the following exceptions:

- Special handling procedures
- Separate Application Integration and Testing (AIT) Lab
- Special Request for Service (RFS)
- Manual Tracking System (excludes the use of the ISF Tools Database)

The Classified Legacy Applications Transition Process and its differences are discussed in Appendix F of this guide.

2.0 OVERVIEW OF LEGACY APPLICATIONS TRANSITION PROCESS

An overview of the NMCI Legacy Applications Transition Process is provided in Figure 2-1. Note the clear distinction between the Rapid Certification Phase and the Risk Mitigation Phase. The Legacy Applications Transition of any site follows the pattern from left to right.

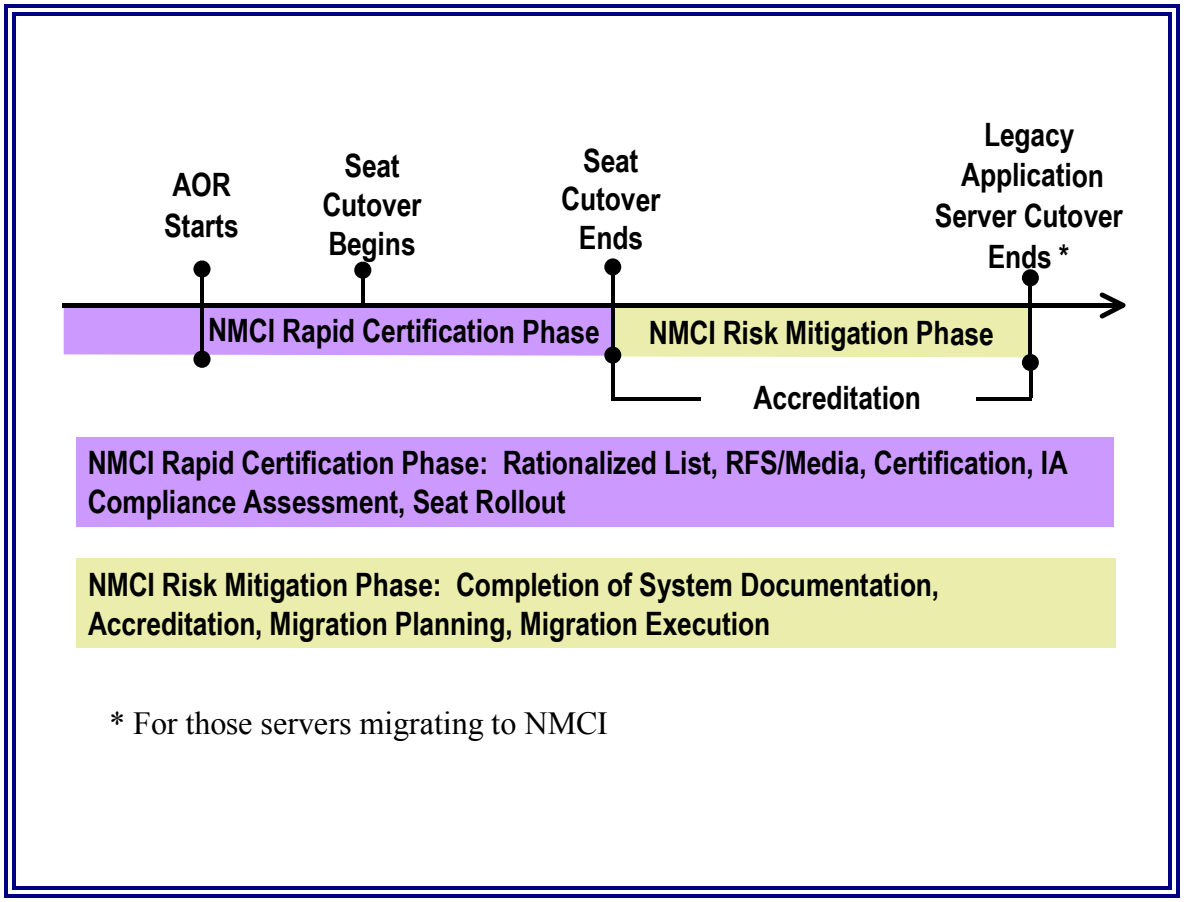


Figure 2-1. Overview of NMCI Legacy Applications Transition Process

The Rapid Certification Phase (purple) includes Assumption of Responsibility (AOR), Seat Cutover (begin) and Seat Cutover (end). Risk Mitigation Phase (tan) begins when Seat Cutover has completed and continues until completion of server migration.

Note the purple and tan bars below the timeline in Figure 2-1. These contain the main portion of information crucial to transition success. All of these are explained in greater

detail in Section 4.0 of this guide. Within the Rapid Certification Phase, customers will become involved with:

- The creation of a Rationalized List of applications
- The submission of RFSs and application media to ISF
- Functional testing of the application
- IA compliance assessment will be completed by the ISF

Within the Risk Mitigation Phase, information regarding system documentation, transition planning, and accreditation will be required. Risk Mitigation Phase is *not* addressed in this document.

Figure 2-2 depicts a more detailed view of the Legacy Application Transition. It breaks down the Rapid Certification Phase into smaller processes describing the 'life of a transitioning application.' Each of the processes will be further discussed in Section 4.0 of this guide.

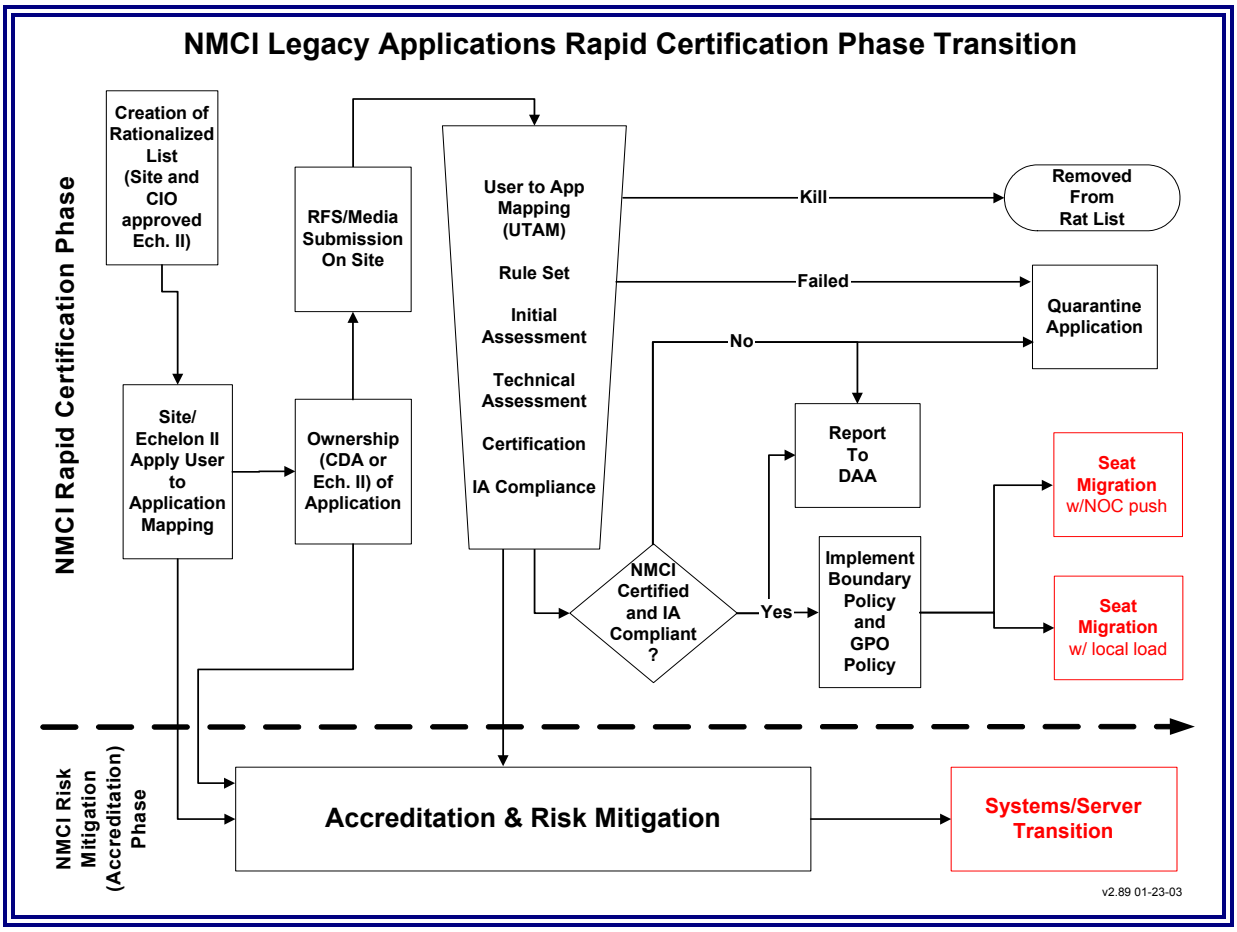


Figure 2-2. NMCI Legacy Application Transition

3.0 ROLES AND RESPONSIBILITIES

The Legacy Systems Transition Process is accomplished using resources of the Navy Information Officer (IO), Functional Area Managers (FAM), Program Management Office (PMO), ISF, Echelon II, Central Design Authority (CDA) and the Command/Site. This section describes the roles and responsibilities of the Legacy Applications Transition Program.

3.1 DIRECTOR NMCI

Director NMCI is managing the acquisition of NMCI. The incumbent works for the Assistant Secretary of the Navy for Research Development and Acquisition (ASN RDA); works within the policy constraints of Department of Defense (DoD) acquisition regulations; and provides additional acquisition guidance to the Navy and Marine Corps NMCI Program Managers (PMs).

3.2 NAVY INFORMATION OFFICER (IO)

The Navy IO is responsible for bringing operational Information Technology/Information Management (IT/IM) requirements into alignment with Navy functionality capabilities using established processes and procedures. The Navy IO advises and assists the CNO achieving network-centric operational capabilities by managing robust global and local networks, employing proven-successful business practices and integrating IT/IM as it applies to warfighters at sea and the supporting shore establishment. The Navy IO also oversees the integration of dispersed sea-based and Joint Command Control architectures, as well as championing the incorporation of industry's significant improvements in IT, in the areas of supply chain and enterprise resource management, into the Navy enterprise.

The Navy IO leads the development of strategic plans and implementation policies for managing global Navy enterprise IT solutions across the Navy. The Navy IO receives requirements from, and provides policies and procedures to, Commander, Naval Network Warfare Command (NETWARCOM) who is responsible for it's implementation.

The Navy IO current focus is on the reduction of Navy legacy applications, supporting rapid transition to NMCI; supporting the establishment of FAMs that will be responsible for all the software applications and databases within their functional area; developing the process for procuring enterprise software licenses for applications that are in use Navy-wide; and leveraging the capabilities of the NMCI to enhance operations and communications within the Navy. In addition, the Navy IO shall be responsible for the following:

- Ensure IT/IM requirements are consistent and compliant with overall Navy/DoD architectures and investment decisions. The Navy IO will work closely with the DON and the U.S Marine Corps Chief Information Officers (CIO) to manage

- Information" and "Knowledge" as key strategic resources in order to satisfy Fleet information requirements.

- Oversee the development and implementation of systems, policies and processes to ensure integrity, availability and authentication; safeguarding of Navy information, and display, processing and storage systems. Substantiate Navy compliance with evolving national security Information Assurance (IA) policies through the acquisition and implementation of approved IT/IM products.

- Establish, manage, and enforce IT/IM configuration standards for hardware, software, and network connectivity. Oversee the development of an enterprise management process for IT/IM configuration control.

- Lead the Navy effort in support to the DoD and DON CIOs' efforts to develop, maintain, implement, and evolve DoD Joint information architectures. Serve as the Navy's lead Point of Contact (POC) for interaction and coordination with other Service, Joint, DoD, and interagency CIOs for implementing the Global Information Grid enterprise solutions.

- Develop, coordinate, and ensure compliance with the Navy's IT/IM Plan that serves as a key input to the IT/IM Strategic Plan. The term "information technology" includes "national security systems" as defined in the Clinger-Cohen Act of 1996.

- Advise the CNO and other senior leadership on all IT/IM-related issues. Key to this function is close coordination and frequent liaison with U.S. Marine Corps CIOs, the Fleet Commanders, Systems Commands, NETWARCOM, and Major Claimant CIOs.

- Support DoD and CIOs' efforts to promote effective and efficient design and operation of information management processes throughout the global Navy enterprise.

- Review and critique all Navy IT/IM Support Plans (C4I Support Plans), prepared and updated at each acquisition milestone in accordance with DoD 5000-series directives, to verify compliance with DoD Joint Technical Architectures and to ensure interoperability, compatibility and integration with other Joint warfighting and support systems.

- Oversee implementation of a Navy-wide IT/IM systems-of-systems testing program to ensure continued interoperability.

- Develop and implement knowledge management strategies that facilitate the improved creation and sharing of knowledge. Knowledge management, which involves delivering the right information to the right decision-maker at the right time to create the right conditions for new knowledge, enables more effective and agile decision-making, resulting in greatly improved mission performance.

- Promote results-based performance measures and best practices to improve mission performance and optimize the return on investment for IT/IM.

3.2.1 Navy Applications Database Task Force (NADTF)

The NADTF was established in March 2002 to act as the focal point for the Navy in developing a reliable inventory of Legacy Software Applications. NADTF is a Navy enterprise organization that is tasked with taking an enterprise view of Legacy Applications in the Navy. The NADTF is responsible for:

- Overseeing Navy-wide Legacy Application identification.
- Coordinating (through PMO San Diego) the entry of needed application information changes into the ISF Tools Database.
- Identifying the Program of Record (POR)/CDAs for Legacy Applications.
- Identifying a standard version for the Government Off the Shelf (GOTS) applications.
- Working with the Program Executive Office for Information Technology (PEO-IT) Enterprise Solutions and DON CIO to identify recommended Commercial Off the Shelf (COTS) application versions so the Navy can acquire required Enterprise Licenses.
- Working with other Navy groups such as Legacy Applications Task Force (LATF), the NMCI Program Office, PEO-IT's Enterprise Solution Office (ESO) and Task Force Web (TFWeb) to obtain synergy and prevent duplication of efforts. The NADTF reports directly to the Navy IO (OPNAV N-7) and the Director of NMCI, to reduce the number of applications that must be integrated into NMCI through:
    - Elimination of inappropriate applications
    - Standardization of application versions
    - Recommending applications be Quarantined if they violate established security parameters
    - Recommending applications be rejected if media is not available at an appropriate time prior to Cutover
    - Providing other recommendations that will enhance the ability to roll NMCI seats while weighing the costs versus benefits to the individual commands

NADTF was established to provide a comprehensive approach for identifying and reducing the number of software applications being used by the Navy. This process was undertaken in cooperation with the NMCI PMO in San Diego and consisted of reviewing the initial application data call that had been entered into the ISF application database, standardizing the naming convention to eliminate duplicate entries, and eliminating

applications and application components that could not operate within the established NMCI Windows 2000 environment. Specifically, the Task Force's objectives were to:

- Identify all Navy software applications and whether or not they would be required to run in the NMCI environment
- Facilitate entry of software application information data into the IST Tools Database
- Take the lead in standardizing software application terminology (name, version, etc.), including being the final authority for establishing the naming convention for all software applications (including version designation)
- Provide recommendations to standardize a limited number of software versions to reduce the number of software applications required to be implemented into the NMCI environment
- Enhance Navy awareness and knowledge of the NMCI implementation process, and
- Provide regular status reports on progress achieved in reducing the number of Legacy Applications to the OPNAV and Secretary of the Navy staffs

As commands commenced the Cutover to NMCI the role of the NADTF changed in response to specific problems that were being encountered during seat rollout. Some of the major initiatives that are underway include:

- Identifying the CDA for each GOTS application.
- Identifying those software applications that are not on the Gold Disk but are widely used throughout the Navy. (The intent is to identify ways the Navy could acquire enterprise licenses to reduce the cost of ownership of these applications for each command and across the enterprise.)
- Assisting the Navy IO in establishing FAM. (The FAMs will be responsible for identifying those applications in each of 23 functional areas that should be established as "standard applications" for use in the Navy.)
- Recommending GOTS and COTS applications (by version) that should be established as standard applications within the Navy.
- Acting as the processing authority for software application waiver requests for applications that are identified and submitted late after Cutover -120, after the commencement of Cutover, and after Cutover has completed.
- Refining the NMCI Legacy Application Ruleset for applications. (This Ruleset determines the criteria that must be met for an application to be permitted to operate within NMCI, which is discussed in Section 4.3.4.3)
- Working closely with the NMCI Designated Approval Authority (DAA) to ensure the NMCI security posture is not compromised by non-compliant applications.

As the rollout of NMCI accelerates and the number of NMCI users increases, it is expected that the role of the NADTF will continue to change in response to user demands. As more experience is gained with the NMCI network, policies and procedures will be established to standardize operating procedures across the Navy and begin addressing the integration of NMCI with other command and control networks within the Navy.

3.2.2 Functional Area Manager (FAM)

Functional Area Manager (FAMs) are responsible for application and database rationalization as described in SECNAVINST 5000.36 (see https://neds.nebt.daps.mil/Directives/5000_36.pdf) FAMs are responsible for enterprise management of applications and databases assigned within their functional area. FAMs are appointed by OPNAV and are responsible for the following:

- Developing and managing IT application and database portfolios
- Ensuring that technology strategies are aligned with business and warfighting strategies
- Researching application and database implementation, certification and accreditation on applicable Navy networks
- Funding and managing the introduction of updates and revisions to the applications and/or databases
- Responsible and accountable for the reduction and consolidation of IT applications and databases within their functional area
- Ensuring metadata and data elements in use are registered and compatible with designated authoritative databases
- Migrating or retiring Quarantined applications and databases
- Working closely with the CIO and the Information Executive Committee Service representatives to ensure that common processes and procedures are consistently used to accomplish this task
- Working with the PORs and CDAs to develop strategies to retire older, obsolete applications and ensure that only current applications are in service
- Identifying COTS for Enterprise Licensing
- Standardizing COTS Applications and Version
- For more information on FAM responsibilities see the Navy Enterprise Application Development Guide (NEADG), http://www.nmci.navy.mil/ or (https://ucso2.hq.navy.mil/n09w/webbas01.nsf/(vwWebPage)/WebBase.htm?OpenDocument&Set=1)

The CIO is expanding the functionality of the current DON Application Database Management System (DADMS) to support the FAM application rationalization process. Each Echelon II command has representatives working closely with the FAM on their applications and databases. Developers and PMs who have questions about the FAM processes should contact their Echelon II Functional Area representative.

3.2.3 Functional Data Manager (FDM)

The FDM is responsible for implementing functional processes to produce and monitor the use of data within and across functional activities, information systems, and computing and communications infrastructures:

- Assist PMs and other system developers in registering system/application (metadata) and data exchange formats and maintaining the metadata baseline
- Develop and maintain Functional Area views of the Data Architecture
- Develop candidate DoD standard data elements in coordination with the respective DoD Functional Data Administrator (FDA)
- Coordinate with applicable stakeholders to ensure DoD proposed Data Standards are usable by Systems
- Designate an authoritative data source for their respective functional areas and maintain the designation in the Application DADMS using processes and procedures approved by the CIO

3.2.4 NMCI Designated Approval Authority (NDAA)

The DAA is a senior policy official who has the authority and the responsibility to make the management decision to accept or not accept the security safeguards prescribed for an Automated Information System (AIS). The DAA is the official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards. The DAA is responsible for:

- Establishing and promulgating the guidelines and security requirements applicable to the NMCI network and the software which operates on that network
- Assuring the fulfillment of the system accreditation for his/her organization
- Ensuring that the AIS security mechanisms enforce the security policy of the organization

3.2.5 Program of Record (POR)

The POR is an office or individual who sponsors and has ownership responsibilities for an application. These responsibilities include but are not limited to funding and maintaining the application. The POR will conduct periodic reviews of their applications to determine if the application is current or requires a more detailed review and update.

POR in conjunction with the CDAs and FAMs must develop a strategy to retire older, obsolete applications and conduct periodic reviews to ensure that only current applications are in service.

3.2.6 Central Design Authority (CDA)

For the purposes of this guide, a CDA is anyone (any organization, site, group, department, division, unit, section, individual, government, or government sponsored contractor) who desires to introduce a new application or change an existing application within NMCI environment. CDAs are responsible for ensuring that their releases are compliant with Navy IA, boundary, and Group Policy Object (GPO) policies prior to deployment within NMCI. CDAs must work with the PORs and FAMs to develop strategies to retire older, obsolete applications and ensure that only current applications are in service. CDAs must keep in mind the requirements for developing and migrating applications that comply with TFWeb, NMCI, Information Technology for the 21st Century (IT-21), Outside-Continental United States (OCONUS) Base Level Information Infrastructure (BLII) architectures, and DON standards.

CDA is also known as Central Design Activity, Central Development Activity, or Commercial Design Activity.

3.3 NMCI PROGRAM MANAGEMENT OFFICE (PMO)

3.3.1 Customer Project Manager (CPM)

The CPM is a government PMO representative to the Echelon II Command/Site in all matters pertaining to the NMCI transition. They are a direct liaison between the NMCI PMO and Flag/Executive Level Claimant Representatives in matters of mitigation and resolution. The CPM's primary mission is assisting the Echelon II in the management and execution of the transition of their Commands/Sites.

3.3.2 Site Integration Lead (SIL)

The SIL is a government PMO representative to the Command/Site in all matters pertaining to the NMCI transition. They are an on-site PMO representative that conduct daily and weekly reports to the CPM, explores granularity of issues, ensures site allocation of resources, etc. The primary mission of the SIL is to assist the Command/Site in their transition to NMCI.

3.3.3 Legacy Systems Division, NMCI PMO

Provide technical resources:

- Provide Legacy Application readiness through oversight during transition and liaison with ISF and Legacy Applications POCs
- Provide data management through testing and Quarantine of applications

- Assist with the development of policies and procedures for Risk Mitigation strategies
- Provide coordination and guidance for Enterprise applications being introduced into NMCI

3.3.3.1 Legacy Application Site Visit Team (LASVT)

The LASVT is comprised of Subject Matter Experts (SMEs) in the Legacy Applications Rapid Certification Transition process. These individuals provide distributed representation to Claimant and Echelon II Level Commands. Duties include:

- Site visits
  - LATG process education
  - NRDDG process education
  - Other process education
- Claimant issue assistance and resolution
  - Rationalization and UTAM process
  - Boundary issues and recommend course of action
  - Assistance in waiver process
  - Interface with other NMCI support activities
  - Interface with NADTF and FAMs
  - Interface with CDAs
  - Coordinate engineering meetings to resolve Legacy Applications and release transition issues
  - Any other special issues as tasked by the PMO

3.3.3.2 Site Transition Execution Manager (STEM)

The STEM is a regional on-site PMO representative who assists with the initial parts of the transition. The STEM assists multiple sites at a time. The STEM is involved with Identification and Rationalization, Collection, Media Submission, Certification and Testing processes (all of these processes are explained in Section 4.0 of this document). STEMs assist and give guidance to the site during these processes to prepare the site for the remainder of the transition. The STEM primes the site for the ISF teams who will transition the site. Five STEM Regional Managers have been deployed to provide STEM Command and Control and regional liaison to the ISF. The SMO and STEM Command Center will provide oversight management, planning, and daily command and control of STEM regional activities.

To prepare the site for transition, the STEM:

- Assists the site with completing the Final Rationalized List on time
- Assists with the collection and submission of RFS & Media
- Assists in scheduling of personnel for Point of Presence (PoP)-in-a-Box (PIAB) / Legacy Application Deployment Readiness Activity (LADRA) testing
- Provides education/training on how to conduct:
  - User-to-App-Mapping (UTAM)
  - Peripheral listing and mapping
- Works with Site on any issues reflected in the ISF Tools Database
- Acts as a liaison between ISF and Command/Site Legacy Application Point of Contact (LAPOC)

Once the STEM has properly prepared the site for ISF to continue transition, the STEM moves on to other sites to assist them as the program executes.

3.3.3.3 STEM Management Office (SMO)

The STEM Management Office and STEM Command Center will provide oversight management, planning, and daily command and control of STEM regional activities. Customers should contact the SMO at the Navy NMCI PMO, SPAWAR PMW-164. The e-mail address for the SMO is legacyap@spawar.navy.mil

3.3.3.4 Enterprise Application Group for Legacy and Emerging (EAGLE)

The Navy PMO created the EAGLE Team, which has three main purposes:

- To provide resources that will focus on the Critical Joint Applications (CJAs) listed in the NMCI contract.
- To provide resources that will focus on the CDA, POR or PM owned applications, with the intent of certifying applications one-time at the enterprise or developer's level rather than re-testing and certifying applications at each individual site.
- Provide resources that will focus on collecting all application related information and provide the focal point for the Site Solutions Engineering (SSE) teams for this information.

The EAGLE Team is divided into three sub-teams:

3.3.3.4.1 Development Approach Team (DAT)

The Development Approach Team is focused on educating CDAs/PORs on NMCI architecture and requirements for developing and deploying applications in NMCI. In

addition, this team will provide guidance in the collection and submission of Engineering Review Questionnaires (ERQ), software media, and CDA RFS documentation for CDA/POR applications. The goal is to produce an enterprise version of each appropriate application and make it available for selection in the Application Catalog in the ISF Tools Database.

3.3.3.4.2 Data Management Team (DMT)

The DMT is tasked with maintaining the ISF Tools Database as the "data repository" for all applications deployed in NMCI. The team oversees accuracy, data integrity, and maintains consolidated application data in one central and accessible location. The team provides tool configuration, data cleanup, and tool maintenance. The team supports all levels of users throughout all steps of the transition process and the CDA submission process. One of this team's primary goals is to reduce the amount of rework required by the CDAs/PORs and by each site team as they come across applications that have been previously encountered.

3.3.3.4.3 Technical Solutions Team (TST)

This team focuses on the more complex POR applications and helps to develop integrated solutions for legacy applications in the NMCI environment. This team can reside at the CDA's location or at the Network Operations Center (NOC) to test CDA applications for the NMCI certification process.

3.3.3.5 Information Assurance Tiger Team (IATT)

The NMCI IATT is the government team consisting of government (civilian and military) and contractor personnel providing technical leadership and IA expertise to government and ISF representatives migrating Legacy Applications into NMCI. It is the responsibility of this team to ensure that the associated residual risk of Legacy Applications to NMCI is understood and minimal. The IATT is under the direction of NMCI PMO and NETWARCOM. The primary objectives of the IATT are as follows:

- Act as an impartial agent of the NMCI DAA and NMCI PMO to ensure Legacy Application migration solutions adhere to acceptable security practices and do not significantly impact Legacy Application operational capabilities.
- Raise the IA awareness of Legacy Application owners, developers, implementers, and users through professional consultation, presentations, workgroups, and relationships with other Legacy Application related teams.
- Ensure the end-state posture of NMCI is not significantly diminished due to the introduction of Legacy Applications into NMCI.
- Provide expertise, guidance, and execution oversight of the Risk Mitigation Phase process of Quarantine Remediation.

The IATT will be responsible for performing the following functions:

- Provide Legacy Applications IA education to claimants, sites, users, and developers. Many of these efforts will be coordinated with the PMO Site Visit Team.
- Provide Legacy Applications IA consulting to the PMO Customer Project Managers. In this role, IATT will act as a single conduit for the CPM regarding Legacy Applications IA.
- Identify, in conjunction with each claimant, the prioritization of legacy applications. This prioritization will be referenced when performing analysis and assigning resources to complete Quarantine Remediation processes.
- Develop, refine and implement the Quarantine Remediation process.
- As part of the Quarantine Remediation process, participate with government leads in on-site Legacy Application reviews, complex Legacy Application reviews, and the development of Legacy Application transition strategies.
- As part of the Quarantine Remediation process, work with sites to submit requests for modifications or exceptions to NMCI firewall security policies.
- Develop (publish) Systems/Server Migration guidance. Develop strategies and work with site in this effort.

3.4 CLAIMANT

3.4.1 Sponsoring Echelon II Command

An Echelon II Command or claimant is defined as an activity that reports to CNO or higher as a normal part of operations. The Echelon II Command is responsible for exercising application management over all subordinate units or organizations. The Sponsoring Echelon II Command is defined as the parent organization of the POR and CDA. As the parent organization the Sponsoring Echelon II Command provides program and content oversight of the applications and releases. The Sponsoring Echelon II Command plays a review and approval role in the Release Deployment Process.

3.4.2 Contract Officer's Representative (COR) or Contractor Technical Representative (CTR)

A government representative of the Command/Site who oversees the NMCI transition for their respective Commands/Sites. Provides government technical interface with ISF and monitors compliance with NMCI contract requirements.

3.4.3 Legacy Application Point of Contact (LAPOC)

The LAPOC is the customer's primary POC for all Legacy Applications transition issues at their Command/Site. The POC works closely with the ISF and PMO to implement NMCI transition.

Customers must identify a primary POC for all Legacy Applications at their Command/Site prior to Cutover -180. The LAPOC should be comfortable communicating with people, knowledgeable of the Command's/Site's IT resources, and familiar with simple databases. The POC works closely with the ISF and PMO to implement NMCI transition.

As the primary site representative for the Legacy Applications transition process, the LAPOC is responsible for:

- Prepare the site for Legacy Applications Transition
  - Coordinate with the STEM, ISF SM, and other Legacy Applications transition personnel (the STEM and ISF SM are discussed later)
  - Review this guide completely and be familiar with its content
  - Obtain access to ISF Tools Database
- Lead Identification and Rationalization effort
  - Create the Identification and Rationalization Game Plan
  - Conduct user surveys for COTS and GOTS requirements
  - Maintain Command/Site's ISF Tools Database entries
  - Deliver Final Rationalized List no later than Cutover -120
  - Create and deliver UTAM no later than Cutover -120
  - Develop and deliver rationalized Peripheral and Driver List
  - Identify Legacy Applications Servers
  - Identify datashares and reachback requirements
  - Create site loadsets
- Lead the Collection efforts
  - Identify Licenses
  - Identify desktop and server connectivity (Network Diagram)
  - Collect Media and supporting documentation in preparation for Submission
  - Lead media submission efforts
    - Submit media and supporting documentation to on-site ISF SM
  - Coordinate Certification, Testing, and Pre-Deployment Efforts
    - Schedule and ensure application owner participation in the testing processes
  - Coordinate post-migration application issues

3.4.4 Application Owner/User

Application Ownership – every identified application will have a designated owner. That owner will either be a formal CDA or a POR or a FAM. If no owner for an application is identified, the application will not be allowed to migrate to NMCI and any reference to it will be removed from ISF Tools.

The application owner/user may be asked to come to the test area to accomplish some usability tests in order to verify that an application is working properly and that it can access the server, datashare, or Web site required.

3.5 INFORMATION STRIKE FORCE (ISF)

3.5.1 Site Manager (SM)

The ISF SM is the lead ISF member at each site. The SM is responsible for the delivery of all NMCI services at the designated location. Service delivery roles include:

- "As-is" support during the AOR period
- Migration/transition support during the Cutover period
- Post Cutover daily production support of existing and new Navy requirements
- Coordinate ISF operations for the site
- Will remain on site for post production
- Liaison to government POCs (CTR)
- Maintains schedule of ISF initiative

3.5.2 Product Delivery Manager (PDM)

The PDM is an ISF resource that works in concert with the ISF SM, to plan, assist, coordinate and execute the delivery of ISF and Government application requirements. The PDM serves as Legacy Systems' resource and delivery manager for claimants and sites they are assigned. The PDM will provide the solutions that aid in the successful migration of applications and systems to NMCI. The roles and other information on PDMs are discussed below.

The PDM serves as Legacy Systems' resource and delivery manager for claimants and sites they are assigned. This includes:

- Planning, tracking, deployment and delivery of those resources, products, or activities that directly support the processing of applications and systems migrating to NMCI
- Serving as the SME for the Legacy Application processing, Legacy Application customer processing, and SSE Team training, planning and deployment

- Supporting the ISF SM and Claimant Manager to ensure that ISF Legacy Systems activities support the sites in the migration of applications and systems to NMCI
- Assisting with the requirements for delivery of applications and the transition of the sites to NMCI
- Ensuring that the sites and other ISF teams are prepared to deliver their requirements in support of site rollout
- Planning, deploying, and managing the resources and tools used for testing, documenting, and delivering applications and systems for NMCI Rollout
- Working closely with the site appointed LAPOC to resolve issues.

PDMs have two main deliverables:

- Site and Resource Deployment Plan - In this plan, the PDM specifies the steps to get the site to Cutover (AOR +60).
- Weekly DAA Summary - This summarizes the progress the site has made with LADRA testing and reports the application's LADRA results. LADRA will be explained later in Section 4.8.

3.5.3 Product Delivery Analyst (PDA)

To assist the PDMs with the numerous tasks they have, each PDM is assigned a PDA. PDAs are physically located at the ISF Commerce Point facility in San Diego. They provide Legacy Application data and other information for management reports, which relies on information extracted from the ISF Tool Database. The PDA provides process support on the submission of Legacy Applications, training, ISF Tools support, data analysis and progress reporting.

PDMs and PDAs will continue to work with a site after Cutover is complete to make sure that the transition is complete and went well.

The ISF PDA is an advisory POC to backup and support the ISF PDM. The PDA provides process support on the submission of Legacy Applications, training, ISF Tools support, data analysis and progress reporting. In addition, the PDAs work with on-site SSE Teams to ensure readiness of applications and associated documentation prior to and during testing. The PDA also works with all members of the Legacy Applications Transition team to ensure proper documentation standards are kept. PDAs interface with government and ISF personnel, including (but not limited to): STEM, PMO, NADTF, DMT, PEO-IT, PDM, SSE Team members, SM, Customer Technical Representative (CTR), LAPOC, AIT, EAGLE and IA Teams. PDA responsibilities include:

- Review, analyze and provide documentation on LADRA readiness and rationalized list status for the Pre-AOR Review
- Create reports for PDMs and ISF Legacy Applications management

- Identify applications submitted that already have a documented NMCI solution (Certification by Association (CBA))
- Provide process guidance and some limited ISF Tools training to ISF and Navy personnel on the submission of Legacy applications and peripherals
- Investigate media and documentation issues (RFS, etc.)
- Participate in recurring site status meetings to provide support and problem resolution
- Conduct Readiness Review (RR) and Post Cutover Assessment (PCA) to ensure readiness of site applications and final status
- Classified PDA is primary POC for creation of Classified Site Workbooks
  - The Classified PDA is the ISF POC for all Classified Rationalized Lists

3.5.4 Site Solution Engineering (SSE) Team Base Lead

The SSE Base Lead is the senior member of the team who coordinates team activities and provides assistance to the SM. The SSE Lead will serve as the on-site representative and spokesman for the team, as well as ensure that any reporting requirements or deliverables are met. Besides serving as Base Lead, this individual will also review the team's deliverables and ensure the integrity of the data and solutions for each application. The SSE Lead is responsible for:

- Interface with site STEM and LAPOC (or the designated Legacy Applications representative) to maintain a loaded queue of POCs to support on-site testing (PIAB, Local Deployment Solution Development and Testing (LDSD&T) or LADRA) activities, when required
- Analyze Site/Claimant-provided list of priority applications for strategic targeting and logical assignment throughout the team
- Monitor team activities and productivity to ensure throughput is optimal and take corrective actions if levels drop below required threshold
- Give guidance and assist the PDM in managing the on-site testing resources to ensure adequate support of team activities
- Provide, update and review daily/weekly reports and team deliverables. Update Project Plan

3.5.5 Site Solution Engineering (SSE) Team Member

The SSE Team Member is responsible for conducting Legacy Application on-site analysis and testing. SSE Team Member will be assigned Legacy Applications by the SSE Base Lead, and will be required to process them according to defined procedures and provide Application Deployment Solution (ADS). Besides processing Legacy

Applications, the SSE Team Member will be required to update the SSE Base Lead daily on status changes for all assigned applications. The SSE Team Member is responsible for:

- Review any available documentation (existing ADS from other sites, or POC provided documentation, etc…)
- Execute the on-site testing (PIAB, LDSD&T or LADRA) as outlined in current process documentation
- Complete an ADS, and provide Base Lead with connectivity, GPO, Network Address Translation (NAT), Domain Name System (DNS) or other requirements for deployment

3.5.6 Application Integration and Testing (AIT) Team

The AIT Team is responsible for packaging and NMCI Certification testing of Enterprise applications, emergent (new) applications, and updates/upgrades/patches/fixes for existing applications. CDAs or an ISF Site Team (Site Solution Engineering Base Lead or Site Transition Manager) are responsible for providing media to the AIT Team for packaging. The AIT Team is responsible for these functions and responsibilities at the San Diego Certification Lab, the Classified Lab at the San Diego NOC and the PoP-in-a-NOC (PIAN). The AIT Team is responsible for:

- Auditing of applications for compliance with the NMCI Ruleset
- Packaging of applications for deployment
- Certification of applications for deployment
- Deploying package to the Novadigm Radia Servers

4.0 RAPID CERTIFICATION PHASE

Figure 4-1 depicts the detailed Rapid Certification Phase process from start to finish. Notice the legend at the bottom right side of Figure 4-1; the colors in the legend correspond to ownership of primary responsibility for completion of the process. For example, the "Media Submission" box is blue, and represents a Government/Site responsibility for completion. Note that many of the processes are tan, indicating a joint responsibility for completion shared by the ISF and the Government.

The overall goal of the Rapid Certification Phase is to work with the ISF to ensure the right applications are available to the NMCI seats of the right people at the right time to ensure completion of the mission and business of the DON. From the customer's perspective, this means many things, including:

- Understanding who uses particular applications at the site.
- Understanding what version(s) of an application are in use at the site.
- Communicating with ISF and PMO personnel to help them understand the applications.
- Communicating with Echelon II NMCI personnel as lists of needed applications are reviewed.
- Making the resources available to accomplish the processes.

Classified Legacy Application

Classified Legacy Application Transition typically follows the steps of the unclassified process described below. The Classified Legacy Application Transition is described in detail in Appendix F.

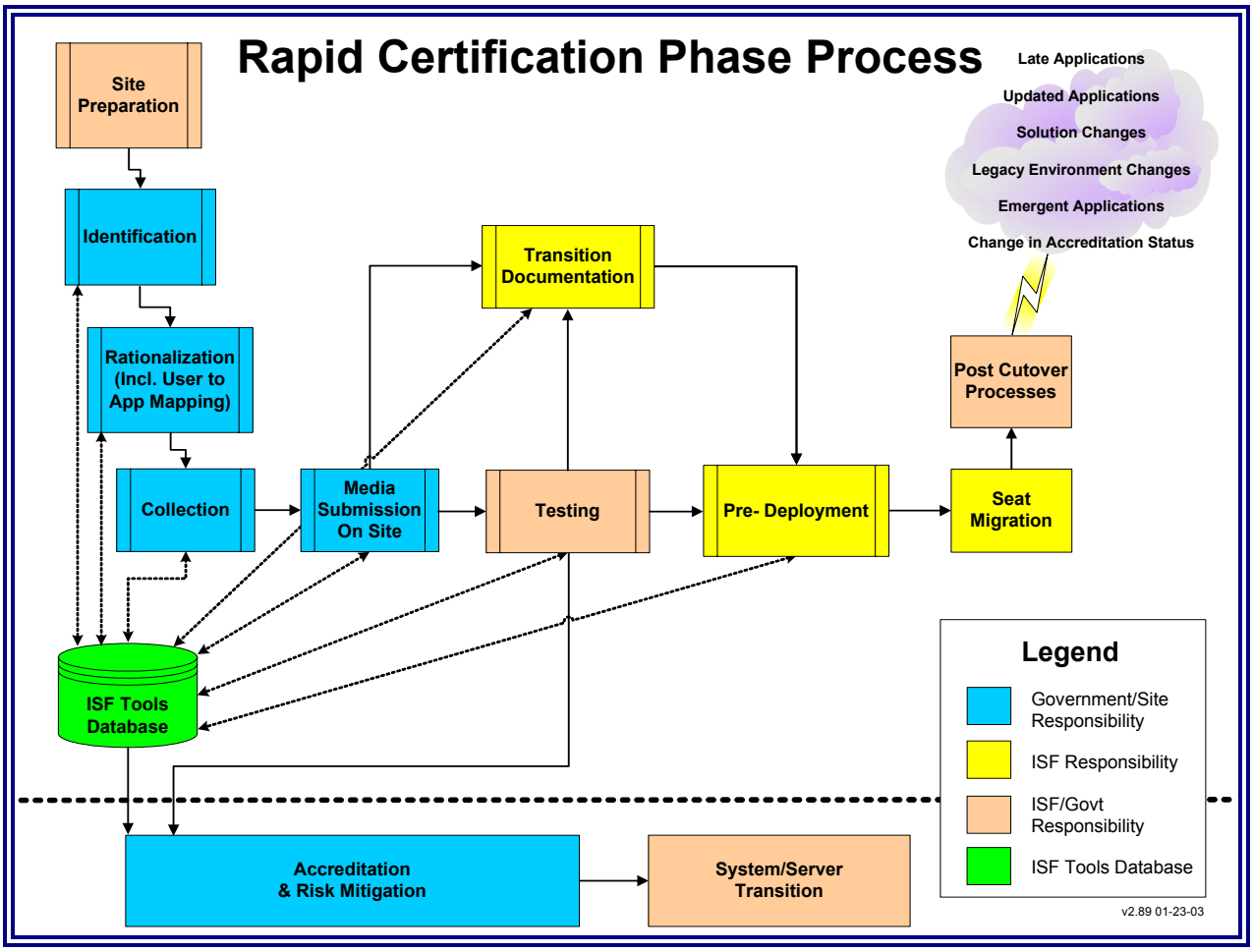


Figure 4-1. Rapid Certification Phase Process

4.1 SITE PREPARATION

Figure 4-2 depicts the details of Site Preparation from the NMCI customer perspective. The activities are designed to get a site ready to start the transition process well before any contractor or Government program management personnel are involved.

Customers should obtain the Legacy Applications Transition Guide (LATG) (this document), read it, and distribute it to all persons at the Command/Site who have an interest in NMCI transition. At a minimum, the Commanding Officer (CO), the IT manager on the CO's staff, the CTR, and the LAPOC should all have copies for reference. Customers should read and understand the overall NMCI Transition processes, which can be found at the following URLs: http://www.nmci-isf.com/transition.htm and/or http://www.nmci.navy.mil/Primary_Areas/Transition_to_NMCI/Index.htm

As part of the site preparation, the following actions need to be accomplished:

- Appoint LAPOC
- Identify Classified Requirements
- Establish contact with PMO and ISF
- Establish ISF Tools Database access
- Obtain the ISF Tools Database Users Guide
- Determine facility Requirement for ISF Testing
- Acquire local IATO for testing connectivity
- Review, accept and assign facilities

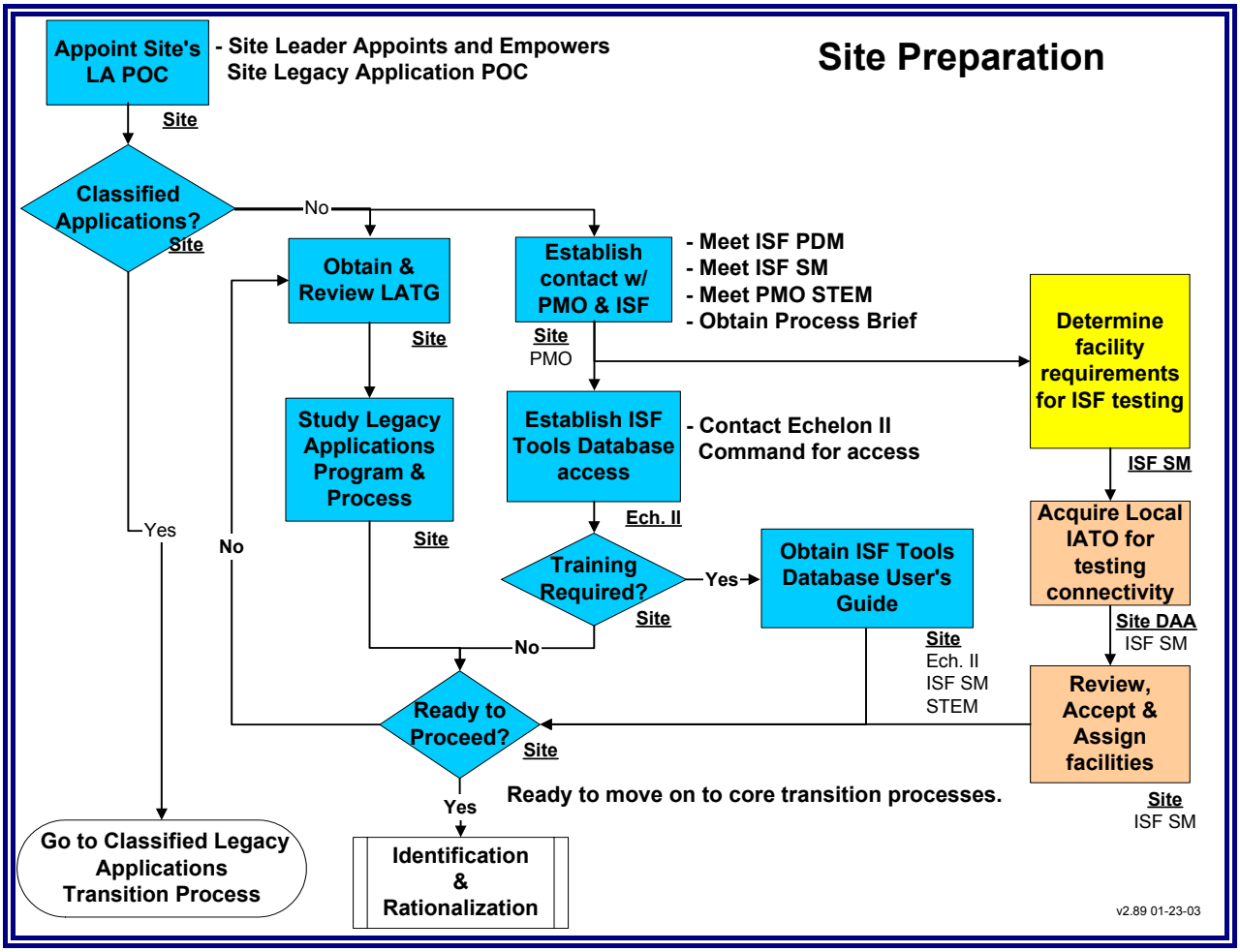


Figure 4-2. Site Preparation

4.1.1 Appoint Legacy Application Point of Contact (LAPOC)

The Site must identify a primary POC for all Legacy Applications at their Command/Site. This LAPOC is knowledgeable of the Command's/Site's IT resources and familiar with simple databases. The POC works closely with the ISF and PMO to implement NMCI transition.

4.1.2 Identify Classified Requirements

Does the Site have classified applications? If yes, proceed to the Classified Legacy Application Transition process, found in Appendix F, for those classified applications. If no, proceed with the Unclassified Legacy Application Transition Process contained in the main body of this guide. If the Site contains both Classified and Unclassified Legacy Application then both processes apply.

4.1.3 Establish Contact with PMO and ISF

The Site will contact the appropriate PMO and ISF Team Members to begin transition of Legacy Applications into NMCI.

- Site Integration Lead (SIL) (Section 3.3.2)
- Site Transition Execution Manager (STEM) (Section 3.3.3)
- STEM Management Office (SMO) (Section 3.3.4)
- Information Strike Force (ISF) Site Manager (SM) (Section 3.4.1)

4.1.4 Obtain ISF Tools Database Access

The Site should contact their appropriate Echelon II Command to obtain access to the ISF Tools Database. Use of this database is mandatory and is critical to a Site's successful application transition effort. All Echelon II Commands have the authority to create user accounts in the ISF Tool Database for their subordinates.

4.1.5 ISF Database Training

If training is required on the use of the ISF Tools Database, the Site should begin by obtaining the ISF Tools Database User's Guide. The User's Guide is available at the following URL: http://www.nmci-isf.com/transition.htm Additional training is available through Echelon II POC or by contacting the EAGLE DMT (nmci-pmo-isftdb@spawar.navy.mil) or by contacting the NMCI Help Desk at 1-866-THE-NMCI.

4.1.6 Determine Facility Request for ISF Testing

The ISF SM consulting with the site determines which facilities will be used for testing the Legacy Application. Customers must identify a suitable location to accommodate a PIAB or NMCI Test Seat. The PIAB is a "mini-NMCI environment" used by the ISF to identify application characteristics. The NMCI Test Seat is an actual NMCI seat used when the NMCI base infrastructure is in place. Deployment of a PIAB or NMCI Test Seat to a site comes later in the transition process, but a prudent site prepares facilities, makes network access arrangements, and understands power requirements in advance of the testing environment's arrival. Further information on the PIAB and NMCI Test Seat can be obtained by contacting the ISF SM and SSE Team.

4.1.7 Acquire Local IATO for Testing Connectivity

The ISF SM works with the Site's DAA to obtain authorization to connect the NMCI PIAB or the NMCI test seat to the Legacy Environment through the NMCI Network. This IATO is for connectivity for hardware and networks and does not pertain to Legacy Applications. This IATO is obtained via the Site and the ISF Network personnel.

4.1.8 Review, Accept and Assign Facilities

The ISF creates a Facilities Site Plan that includes recommended square footage, power requirements, environmental requirements, and cable requirements as well as computer hardware. The plan is provided to the site for review and acceptance. Negotiations between the ISF and the site may occur. Once the Site and the ISF reach agreement, the facility's Plan will be implemented.

4.1.9 ISF Tools Database

The ISF Tools Database has been developed to record and share collected information about software applications to be deployed in NMCI. It is the authoritative source for all Legacy and Emerging Applications in NMCI. ISF Tools will collect all information related to Legacy Applications Transition, specifically:

- Site Preparation
- Identification
- Rationalization
- Collection
- Media Submission
- Testing – Packaging and Certification
- LADRA test results and Quarantine status during Pre-Deployment

The ISF Tools Database is also the authoritative source for testing and deployment information for Legacy Applications, where users can:

- Record all of their Legacy Applications.
- View Application Catalog.
- Develop their list of Legacy Applications and submit their Rationalized List.
- Create a RFS for Legacy Applications.
- Monitor real-time status of Legacy Application proceeding through the transition process.
- Create reports such as a site's Workbook showing all rationalized Legacy Applications and their status in NMCI.
- View NADTF and FAM approval status.
- View Application waiver status.
- Identify and track Quarantined applications.

Further information on the ISF Tools Database is available online at the following URL: http://www.nmci-isf.com/transition.htm

4.1.10 DON Application and Database Management System (DADMS)

DADMS has achieved initial operational capability. DADMS will contain a complete inventory of all authorized applications and databases residing on all Navy networks (e.g. NMCI, IT21, and OCONUS BLII). Customers should understand the difference between DADMS and the ISF Tools Database. DADMS is not NMCI-specific and cannot be used to monitor or facilitate NMCI Transition status. Use of the ISF Tools Database, on the other hand, is mandatory in connection with NMCI Transition activities.

4.1.11 Site Ready to Proceed Core Transition Processes

Once the preparatory steps have been completed, the site proceeds to Identification and Rationalization.

4.2 IDENTIFICATION

Figure 4-3 depicts the Identification process. The customer's goal in Identification is to inventory all Legacy Applications needed to conduct their business after transition to NMCI. The Identification and Rationalization processes are important Government responsibilities. While the Echelon II Commands are responsible for oversight of these steps, much of the execution occurs at customer's sites. Experience with early implementers of NMCI confirms the value of being proactive. The first increment of customers indicated sites should begin these processes well in advance of 180 days before Cutover. Do not wait for ISF or PMO personnel to arrive on-site for this work to begin.

As part of the Identification process, the following steps need to be accomplished:

- Create the Identification and Rationalization Game plan
- Socialize Site's Game Plan and Strategy
- Concurrent Process
  - Survey users for GOTS Requirements
  - Survey users for COTS requirements
  - Create user list and begin UTAM
  - Create Site loadsets
  - Gather in use peripherals and drivers
  - Identify Legacy Applications Servers
- Identify Datashare and Reachback

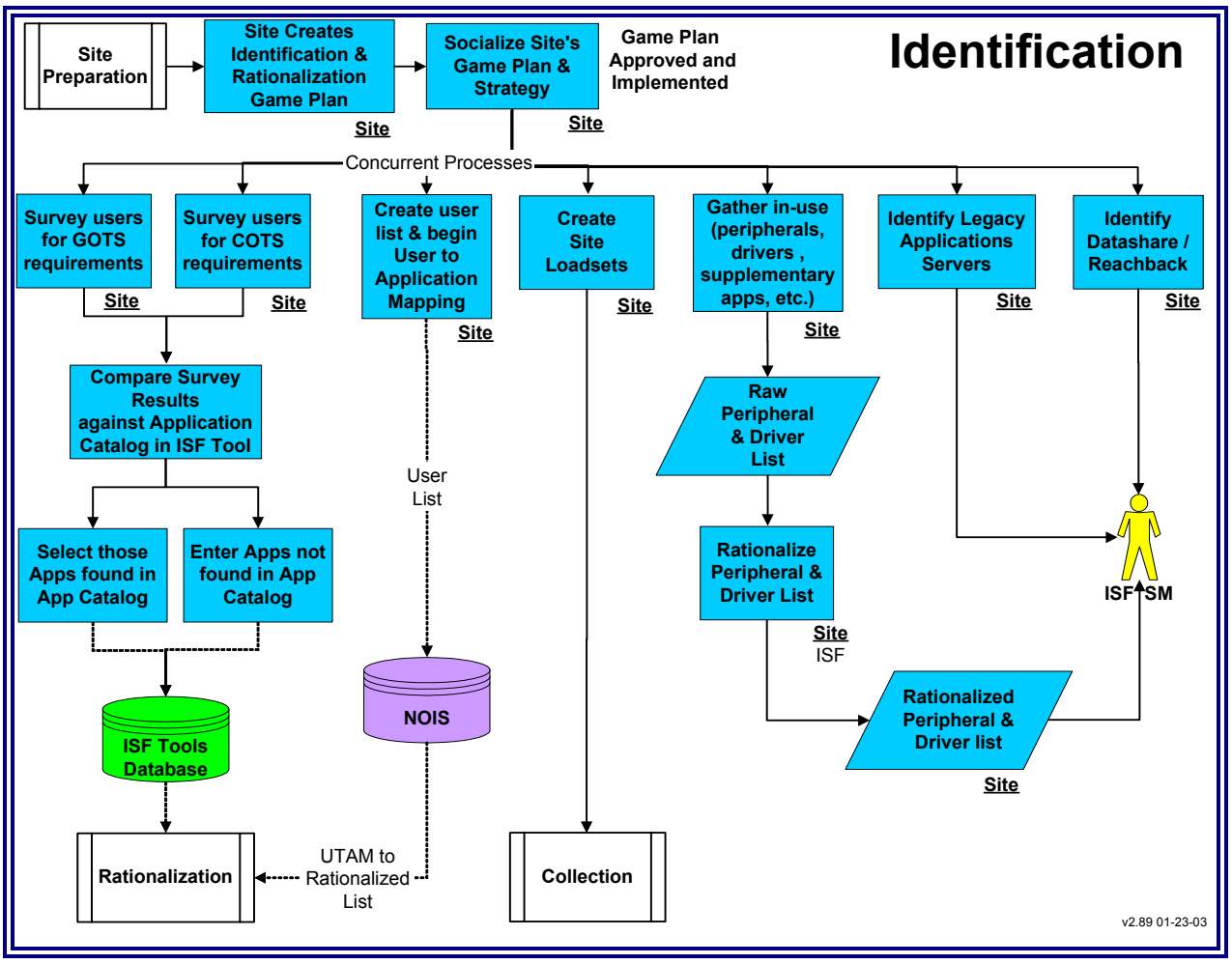


Figure 4-3. Identification

4.2.1 Create the Identification and Rationalizion Game Plan

Customers should create and implement an Identification and Rationalization "Game Plan." This plan specifies who at the site is responsible for each of the tasks associated with the identification of Legacy Applications, as well as other critical information related to NMCI transition. There is no set format or template for the site's game plan. The key individuals selected by the site must meet, communicate, and formulate a viable plan that can be easily coordinated and implemented.

When the plan is implemented, there are many types of information that will be identified. This includes:

- Identification of the GOTS applications that will be required in NMCI.
- Identification of the COTS applications that will be required to run in the NMCI environment.
- Identification of the of mission essential website URLs used by the site.
- Creation of the initial UTAM list.
- Identification of desktop legacy peripherals, drivers, and associated software.
- Identification of the Legacy Application servers.
- Identification of the Datashare and Reachback requirements for the Legacy Applications.

4.2.2 Socialize Site's Game Plan and Strategy

Once the Command/Site has created a game plan and strategy for identifying and rationalizing Legacy Applications, the plan will be circulated amongst the appropriate staff.

4.2.3 Concurrent Process

4.2.3.1 Survey Users for GOTS/COTS Requirements

The LAPOC at the customer site will ensure that a survey is conducted for the GOTS and COTS operational requirements. All users should be surveyed to determine their COTS and GOTS requirements. There is no set procedure, format or template for conducting this survey. Each Command/Site must develop methods based on their needs. Tools such as Altiris Asset Management Suite, Microsoft SMS and Belarc advisor are examples of tools commercially available to automate the process. Once the application requirements are collected and compiled, they are entered into the ISF Tools Database.

4.2.3.1.1 Entering Identified Applications into ISF Tools Database

The LAPOC ensures the site compares the entered applications against the application catalog found in the ISF Tools Database. Any identified/surveyed found in the Application Catalog in the ISF Tools Database will be selected by the Command/Site for

inclusion into the Command's/Site's Rationalized List. Any surveyed applications not found in the Application Catalog in the ISF Tools Database must first be entered into the catalog by the command/site's Echelon II LAPOC Workflow Manager or the application CDA/POR POC prior to linking the Application to the Rationalized List.

If applications are selected from the Application Catalog, they will be shown as "above the line" in the Rationalized List. Those applications not selected from the Application Catalog will be shown as "below the line" in the Rationalized List until an approved waiver is received. "Above the line" indicates applications that are accepted, rationalized and ready for transition into NMCI. "Below the line" indicates applications not approved or awaiting approval for transition into NMCI. Waiver approval to move an application to the "above the line" status resides with NADTF and the FAMs.

4.2.3.1.2 Selecting the Central Design Authority (CDA) Version

When the LAPOC is entering the identified applications into the ISF Tools Database, one of the initial steps is to search the application catalog by acronym or common application name. While in the catalog, a check should be made for the "CDA version" of the application being entered. LAPOCs should make every effort to utilize the CDA version found in the catalog. The CDA version is the latest and only approved version of the application. The CDA version is highlighted in the catalog and has an RFS number followed by "-CDA". For example the CDA version for application ACMEAPP would show as "12345-CDA". The CDA version in the catalog has been certified for use in the NMCI environment. By selecting this version, the LAPOC is performing a CBA to that application and must follow the steps for CBA found below. In addition, selecting the CDA version will accelerate and streamline the process of application rationalization, collection, submission, and certification for the site.

If applications are requested are not in the catalog, they must be entered by the appropriate owner (CDA, POR, FAM).

4.2.3.1.3 Creating a Rationalized List in ISF Tools

The list that identifies what applications commands desire to have transitioned into NMCI is known as a Rationalized List. Creating a Rationalized List is essentially a three-step process consisting of linking applications from the application catalog to the command's UIC, creating a RFS for each application, and linking the application to each Implementation Group where the application will be tested and deployed. A command starts by linking each desired applications from the application catalog to its command name and UIC. A command has the option of creating a single Rationalized List under its Echelon II's UIC in order to manage applications centrally, or an Echelon II may direct commands on which UICs to use for creation of creation of Rationalized Lists. Once the correct UIC is determined, commands can link applications to it from either the application catalog page or the rationalized list page. It is very important to correctly identify applications by long name, acronym, and version. Application records with unknown version numbers will result in automatic FAM and NADTF disapproval.

Again, if a desired application is not found in the catalog, LAPOCs must contact their Echelon II LAPOC Workflow Manager or the CDA/POR of the application to have it added to the catalog.

4.2.3.2 Create User List and Begin UTAM

The process of associating applications to Users or to client machines is known as UTAM. UTAM starts as soon as the Legacy Applications Transition process begins. It is highly recommended that sites collect UTAM information as they are performing the early steps of identifying and collecting Legacy Application data. Application mapping information will assist in application rationalization by identifying user demand. This transition step is important to ensure that applications are mapped to users or to their desktops

This transition step is critically important to ensure that applications are mapped to users or to their desktops.

Failure to perform this step adequately and early in the transition process will result in users not having access to their needed applications at the time of seat rollout. An application not mapped to either a user or a machine will result in unnecessary LADRA testing and will result in applications being disapproved by NADTF. Lessons Learned have shown that over 50% of submitted applications had no user associated when it came time to install the application. Working on these unneeded applications wastes resources, assets, and time.

The Initial UTAM must be completed during the Identification Process. The Initial UTAM will be used as a reference when reconciling the Initial Rationalized List at Cutover -180.

The UTAM is continually refined during the Rationalization and Collection Processes. The Final UTAM is due at Cutover -120. The Final UTAM will be given to the ISF SM for delivery to the ISF Transition Team for use in building User Profiles and the Active Directory. Applications that do not show a user mapped to them will be removed from the list.

It is understood that Commands/Sites will experience changes to their Final UTAM after the Cutover -120 delivery. It should be expected that some changes will occur as personnel change billets, transfer, etc. The ISF requires the Pre-Cutover UTAM 30 days prior to Cutover for final changes to the User Profiles and the Active Directory to make Cutover. Additional changes to the UTAM after this point will be handled at the discretion of the ISF Transition personnel. The ISF is not required to address these late changes until Cutover is complete.

Note: NMCI in its present configuration actually requires “application to seat” mapping. Since users and their profiles are assigned to particular seats, applications must be

mapped to the profiles assigned to those seats. Until users are allowed to use any NMCI desktop with a "roaming profile", UTAM will actually be "application to seat" mapping.

4.2.3.2.1 NMCI Ordering Interface System (NOIS)

UTAM is accomplished using the NMCI Ordering Interface System (NOIS). NOIS automates the UTAM process by tying the users listed for seat orders to the applications identified in the ISF Tools Database.

If NOIS is unavailable, UTAM becomes a manual process using a spreadsheet to design the associations between the user and their applications. Appendix G.5 depicts the 1-app-per-user-line-format that UTAM submits.

NOIS is a DON single point-of-entry system that:

- Captures:
  - User profile data
  - As-Is inventory details
  - User level seat requirements
  - User level legacy application and peripheral mapping
- Provides an automated interface to ISF eMarketPlace system for task orders
- Supports the deployment of NMCI seats throughout the DON

The NOIS Website can be found at: https://nois.navair.navy.mil

4.2.3.3 Creating Application Load Sets and Standardized User Profiles

In an effort to streamline deployment of applications and standardize usage of applications, applications on a Command/Site's rationalized list can be grouped into either Load Sets or Standardized User Profiles using the Application Template feature found in ISF Tools on the Rationalized List page. Load Sets and profiles are standardized groupings of Legacy Applications built around organizations, seats and users. Common grouping of applications that are to be deployed to either all or a group of NMCI seats are known as Load Sets. Load Sets can be assigned to groups of seats according to organization or to location. Applications that are grouped according to user roles, e.g., admin or finance, are known as Standardized User Profiles and can be assigned to groups of users based on user roles and attributes. These groupings can be developed during UTAM and will expedite deployment of applications to the desktop, while maintaining flexibility for each Command/Site to ensure the users have the applications they need. Further, profiles assist in the Command/Site's management of its software and applications.

Legacy Application Profiles are built around roles, which are the specific applications necessary for a user to perform his or her job. Profiles are the end result of mapping the applications to the user. They represent the groupings of applications that will be placed

on each user's machine. These applications range from general Windows applications to the unique Legacy Applications specific to the user's billet or position. If UTAM is completed properly, profiles will be relatively easy to complete. Each user will have a list of the Legacy Applications they need. These roles will be combined with the loadsets to create the user's profile.

A loadset is based on creating a standardized grouping of applications around particular sub-sets or organizations of the DON. Common applications used by everyone in a sub-set, discovered during UTAM, will be incorporated into a loadset. Loadsets consist of Enterprise Licensed Applications appropriate for all NMCI seats in this sub-set. A sub-set could be anything from the Navy or Marine Corps overall, down to a base, station, or site. For example, in the same manner the Gold Disk is for all NMCI users, a Blue Disk could be for the Navy, a Green Disk for the Marine Corps, a Purple Disk for Joint Applications, and a Silver Disk for Allied Applications, etc. Loadsets can continue further down to any component of the Navy or Marine Corps, or any component of a command/base/station/site, such as departments, divisions, wings, squadrons, battalions, units, etc. Loadsets can be designed to contain the loadsets of subordinate organizations.

Loadsets are used to make up much of a user's profile. Any applications for a user not included in the loadsets will be added into the profile. For example, a Navy Administrator's profile could consist of the Gold Disk, the Blue Disk, loadsets for the organization the Administrator is at, and then any other applications the Administrator needs to do his or her job that are not included in the loadsets.

Grouping applications is accomplished by simply clicking on the 'Create Application Template' button in the ISF Tool. In the popup window that appears, a name can be assigned to the template and applications can be assigned by selecting applications from the list in the right-hand column and clicking on the 'arrow' button to place them in the left-hand column. Applications can be added and removed from the template by toggling between the left and right columns using the arrow buttons. When finished, click on the 'submit' button.

Application Templates automatically appear at the top of the Rationalized List. They can be updated by clicking on the template name link.

When mapping applications, an Application Template automatically maps the applications contained within. Simply map the name of the template to seats or to users in NOIS.

Commands/sites are encouraged to design Loadsets and Profiles as much as possible to streamline the application testing and deployment process. Lessons learned from previous sites have indicated that loadsets and profiles are the key to successful Cutover.

4.2.3.4 Creating a Request for Service in ISF Tools

The second step, after linking an application to a rationalized list is to create a Request for Service (RFS) for each application on the list. An RFS is an ISF document used to identify a legacy application requirement and collect necessary information for application packaging, certification and LADRA testing. There are three kinds of RFSs: a CDA RFS, a command-level RFS and a site-specific RFS.

Only an application's CDA, vendor, or program manager creates a CDA RFS. The existence of a CDA RFS is easily determined when looking up an application in the application catalog. Alongside the application record is a CDA/POR link that displays POC information for a CDA RFS. Clicking on the usage link found alongside the application record and then clicking on the CDA RFS link that appears in the popup window can view the CDA RFS itself.

In some cases, when a CDA RFS exists, a command will not be required to submit its own command-level or site-specific RFS. A command will automatically inherit the CDA's RFS number when linking an application to its Rationalized List.

In most cases, however, a command-level RFS is required. A command-level RFS is created by clicking on each of the 'Create RFS' links found on the right-hand side of the Rationalized List page. The RFS form appears in a popup window displaying the necessary data fields to be populated. When finished, click on the submit RFS button and an RFS number is automatically assigned. If changes are required, the RFS can be updated by clicking on the RFS number. An RFS can be updated only while it is in 'RFS Submitted' status. Once the Application Integration Testing (AIT) lab begins work on an application, its RFS can no longer be updated by the command submitting it.

A site-specific RFS is used if an application requires specific local information and POCs for local LADRA testing. The steps to create a site-specific RFS are the same as creating a command-level RFS except that it must be created after the application is linked to an Implementation Group. After an application is linked to its Implementation Group, click on the 'Create IG-Level RFS' link. If an application already has a Command-Level RFS number, the IG-Level RFS number will replace it automatically. Linking applications to Implementation Groups is explained in the next paragraph.

4.2.3.5 Linking applications to Implementation Groups in ISF Tools

The final step in creating a rationalized list is to link applications to their respective Implementation Groups. An Implementation Group refers to the site where applications will be tested and subsequently deployed. It is the name given to the workbook used to record LADRA test results and DAA report data. An Implementation Group name consists of the official ISF site name and schedule increment.

Site names are defined and maintained by ISF and held in ISF Tools, which can be viewed under the 'Admin' tab and 'Implementation Group' link. It is important to note

that site names are based on actually military installations, e.g., naval bases, naval air stations, air force bases, army posts, etc., or they are based on leased commercial spaces or buildings that contain a command or activity, e.g., Crystal Gateway 4, Crystal Park 3, etc. Sites are not based on city and state. Each site name is assigned a unique four-character identification code. These four-codes and site names are used throughout NMCI for a variety of purposes including naming network topography, i.e., seat and server farm names; specifying delivery locations for seat and CLIN orders in NOIS and eMarketplace; and, in the enterprise seat rollout schedule. Increments are used in the enterprise seat rollout schedule to define groups of commands and seats to be rolled out at a given site at a given time.

An example of an Implementation Group is the following: applications to be tested and deployed at the site Washington Navy Yard in the 40K seat plan schedule increment would be linked to the Implementation Group name Washington Navy Yard – Increment 40k.

To link applications to Implementation Groups, first render the desired Rationalized List. Then click on the desired Implementation Group in the 'Impl Group' pull-down field at the top of the Rationalized List page. The EAGLE Data Management Team assigns the choices available in the 'Impl Group' pull-down.

4.2.3.6 Gather In-Use Peripherals and Drivers

A peripheral is any device that is connected to or works in conjunction with a workstation/desktop. Legacy peripherals are those peripherals not turned over to the ISF as part of AOR. There are legacy desktop peripherals, which are connected to a single NMCI seat and sit on a desktop, and there are legacy network peripherals that are standalone units connected directly to NMCI and multiple NMCI users share them. Examples of legacy peripherals include printers, scanners, plotters, chart-makers, Personal Digital Assistants (PDAs), digital cameras, zip drives, CD-RW, etc.

A peripheral is any device that is connected to or works in conjunction with a workstation/desktop. Examples include printers, scanners, plotters, chart-makers, Personal Digital Assistants, digital cameras, zip drives, CD-RW, etc.

Drivers are the associated software designed to allow the peripheral to function with the workstation/desktop. They may be defined as:

- Software that interfaces with a computer to a specific peripheral.
- A device driver is the associated software designed to allow a peripheral to function with the workstation/desktop. There are device drivers for printers, displays, CD-ROM readers, diskette drives, and so on. A device driver essentially converts the more general input/output instructions of the operating system to messages that the device type can understand.

Note: Peripherals and their drivers are not part of ISF Tools Database nor included on the Legacy Applications Rationalized List. They are not ***applications***. ISF doesn't certify drivers or peripherals, only applications.

4.2.3.6.1 Peripheral Support Software

Sometimes there is software associated with peripherals to support the hardware. This supporting software is not a driver, but an application associated to support the peripheral. For example, a chartmaker may have support software that enables the user to make charts (i.e., Enterprise Systems Chartmaker will have the Enterprise Systems Chartmaker Design program with the actual chartmaker). This software should be listed on the Rationalized List and submitted for certification and testing as an application

4.2.3.6.2 Bundled Peripheral Support Software

Sometimes, the driver and support software are combined into one complete package in support of the peripheral. This is referred to as bundled software. In this case, the bundled software is listed on the rationalized list and submitted for certification and testing as an application using a single RFS. The contents of the bundle should be listed in the *Additional / Special Instructions* section of the RFS, as well as the legacy peripheral for which this RFS is intended..

4.2.3.6.3 Peripheral Categories

There are two categories of peripherals: (1) customer/user owned and (2) NMCI contract provided. For those peripherals ordered and provided by the NMCI contract, the devices, drivers, and their maintenance are included with the peripheral order. Legacy Peripherals are those devices that are provided by the customer/user. Procurement and maintenance of Legacy Peripherals and their associated software/drivers are the responsibility of the customer/user. However, the ISF maintains an extensive library of peripheral drivers and may be able to provide the appropriate driver. ISF will not require drivers if they are easily downloaded from a website or already included in the Windows 2000 Operating System. The site should be prepared to deliver drivers if required. Non-driver software that is associated with a peripheral is considered a Legacy Application and is to be handled as such in accordance with this guide. Legacy Peripheral installation is a customer/user responsibility, while connectivity and driver installation are the responsibility of the ISF.

4.2.3.6.4 Rationalized Peripheral and Driver List

The site must provide the ISF with a list of their Legacy Peripherals and their associated drivers. This is necessary to ensure the ISF will provide connection for the peripherals and, since the desktop is locked down, provide installation for the associated driver. The Site Representation of Legacy Peripherals is a list in a spreadsheet format. The template is provided in Appendix G.1. The list of peripherals and their associated drivers are turned over to the ISF SM. The list of these components is not part of the Legacy Applications Rationalized List in the ISF Tools Database. The Site delivery of the

Peripherals and Drivers Rationalized List to the ISF SM starts the internal ISF evaluation and rationalization of these items.

4.2.3.7 Identify Legacy Application Servers

4.2.3.7.1 Legacy Server

Legacy Servers are those systems that include existing customer software and hardware currently in use at a site by people performing the mission or business of the DON that are not included in the NMCI standard services or the CLIN catalog. Legacy servers may be individual servers hosting one or more applications or systems consisting of multiple servers, console/workstations, supporting devices/systems and possibly network devices. Current legacy servers may run any of several possible operating systems (including, but not limited to, Windows 2000, Windows NT 4.0, Solaris, HP-Unix, Mac OS, Novell) and may host server as well as client applications and agents.

4.2.3.7.2 Identifying Legacy Servers

The site must identify their Legacy Servers to the ISF to ensure that the ISF Transition personnel can properly map the desktop to server connection. This list is usually generated using a spreadsheet and delivered to the ISF Site Manager. A template example of this deliverable can be found in Appendix G.8.

4.2.3.7.3 Server Only Operating Systems, Applications and Tools

Non-Windows 2000 Legacy Application Server operating systems (for example: Solaris, HP-Unix, Novell, Linux, Windows NT, MAC OS, etc.) will not be included on the Legacy Applications Rationalized List nor tested in NMCI. For migration into NMCI, servers with non-Windows 2000 operating systems will need to interface with the NMCI Windows 2000 backbone.

Server tools that will be loaded to NMCI desktops need to be listed on the Legacy Applications Rationalized List and submitted for NMCI testing. Sun Net Manager, HP Openview, TNG Unicenter, and Peregrine IND are examples of server tools that have administration clients that can control servers externally from a desktop. The client end of these tools will be identified and submitted for NMCI testing. Such server tools can be left alone on the server and in that configuration, will not require NMCI testing.

NOTE: Some of these tools have the option to use agents; however, agents are not authorized for use in NMCI per the NMCI Application Ruleset.

4.2.3.8 Identify Reachback and Datashare

In order for the ISF to properly map and route users and their machines to servers, files, databases, etc., the site must identify all reachback and datashares requirements. NMCI will replace all existing Legacy network operating system and electronic mail servers.

However, legacy applications, files, datashares, databases, servers, etc. will still exist and must be mapped to the new NMCI desktops. Therefore, for a successful transition, specific reachback requirements must be identified to the ISF to ensure they will be included in the transition.

Appendix G.7 provides a template for use in identifying datashare and reachback requirements. Other network methods such as *tracert* and *traceroute* can be used to identify network connections and their associated IP Addresses. However, you should consult your network manager prior to use.

4.2.3.8.1 Reachback

Whether working in NMCI or the Legacy environment, users need constant access to a vast array of network drives, peripherals, databases, data stores, networks and services to accomplish their jobs. In the Legacy environment these service connections were simplified, over time becoming a generic consequence of the way of doing business. However, with the migration to NMCI, many of them will not initially transition with the user, so some provisioning or Reachback will be required to link them through the Boundary 2 (B2) into the Legacy BAN or through the Boundary 1 (B1) to other legacy assets. The concept of Reachback as it relates to NMCI is that users must identify all paths, connections and interfaces employed in mapping their NMCI seat back to other legacy drives, databases, servers and networks. Systems Administrators will be able to properly map/reroute those services through the B1 and B2 until such time as the optional services themselves can be migrated into the NMCI enclave. To ensure users have uninterrupted access to the services and resources they need, it is vital that the LAPOC properly identify and document all service paths and connections associated with each seat during the Identification phase of the Rapid Certification process.

4.2.3.8.2 Datashare

Datashares act as repositories and central access points for a continuously evolving number of datasets. This arrangement ensures greater reliability and flexibility while increasing overall accuracy and maintainability. The datashare may represent the actual data resource residing in a shared file, optional drive, shared drives, database, server, library, network, or legacy environment.

For NMCI, users need constant access to their datashares, especially during transition, when the datashares will exist in the legacy environment. Access to these assets must be guaranteed to ensure continuity of business practices. The LAPOC must ensure that all datashares are identified, documented and submitted to the ISF. The ISF must ensure the new NMCI seat is properly mapped to the datashares. This may include reaching across the NMCI boundaries (1 & 2).

4.2.4 Late Identification

Customers must identify their Legacy Applications on time. Per CNO Naval message of 30 September 2002 (301245Z SEP 02), all applications were to be identified and entered into ISF Tools Database by 29 November 2002. Legacy Applications identified after this time are considered "late." Lateness jeopardizes their inclusion in seat Cutover. However, if the application is identified before the specific site Cutover date it is still considered Legacy and will be transitioned by the ISF per the contract.

Applications identified after the start of Cutover are considered "emergent." Emergent applications are not considered to be Legacy Applications based on the NMCI contract terms. The Command/Site and/or the Echelon II Command will be responsible for the financial implications associated with NMCI Certification and transition of emergent applications. Please refer to Appendix C for further details of the Late Application Identification and Submission Process.

4.2.5 Implementation Groups

ISF Tools uses Implementation Groups for defining groupings of transitioning Commands/Sites by geographic locations. Commands can exist at multiple geographic locations. Commands can have subordinate activities that exist at different geographic locations. Implementation Groups consist of one or more activities from one or more claimants. Each subordinate activity or command located at a specific geographic location (Site) is assigned to an Implementation Group, which represents their physical location.

Commands creating Rationalized Lists in ISF Tools may select to create a Centralized Rationalized List. One instance for generating a Centralized Rationalized List is to allow a Command that does exist in multiple geographic locations to utilize a single Rationalized List.

Another instance for generating a Centralized Rationalized List is to allow multiple subordinate activities existing under the same command to utilize a single Rationalized List. In either instance, a Command level RFS can be submitted for each application contained within the Centralized Rationalized List.

4.3 RATIONALIZATION

Figure 4-4 depicts the Rationalization process. The goal in Rationalization is selecting only those desktop and server-based applications, both COTS and GOTS, required to support command or DON missions, goals, and business processes.

After the Legacy Applications have been identified, the information is carefully examined, scrutinized, and analyzed by the Command/Site for rationalization. Rationalization consists of categorizing the applications by type and functionality, and then applying NMCI policies, rules and Navy/Echelon II/local standards to eliminate

those that violate the rules and standards. The customer is encouraged to eliminate any unnecessary, redundant, or nonstandard applications that are not absolutely required to support the site's mission, processes, and goals.

General Notes on Rationalization

Rationalization of Legacy Applications is not dependent on completing the Identification steps. Rationalization can occur concurrently with the Identification steps. Customer decisions on the disposition of applications (e.g., eliminate, consolidate) can occur as soon as sufficient information becomes available. Additionally, rationalization may (and ideally should) be independent of the NMCI transition process. However, NMCI transition provides an excellent opportunity to achieve the objectives of the rationalization process.

Echelon II Commands must help determine which applications should be retained in service. Echelon II Commands are expected to review all subordinate Command's/Site's rationalized lists for approval. They must formally approve the Final Rationalized List in the ISF Tools Database by indicating those accepted applications as rationalized. A Command's/Site's Rationalized List will not be accepted until it has been reviewed and approved by the Echelon II Command.

The end state of this effort is the submission of the Final Rationalized Legacy Application List via the ISF Tools Database. Any additions to the Rationalized Legacy Application List after 29 November 2002 will require NADTF approval.

Navy Message R 301245Z SEP 02 CNO WASHINGTON DC ENTERPRISE STRATEGY FOR MANAGING NMCI APPLICATIONS AND DATABASES directs action to achieve common operational picture of the Navy's applications and databases in DADMS and the continued use of the ISF Tools Database as the primary tool for ordering and implementing applications in NMCI. This message:

- Directs all Echelon II Commands to ensure their Final Rationalized List of all NMCI applications is reflected in the ISF Tools Database within sixty (60) days of the date time group of this message (29 Nov 2002)
- Requires the approval of the applicable FAM and Navy IO for the subsequent addition of applications to ISF Tools Database by Echelon II Commands and subordinate Commands
- Mandates that every Navy application will have a designated CDA and/or owner identified by name with contact information
- Specifies a process to be followed to track all Quarantined applications

NOTE: If no owner for an application is identified, the application will not be allowed to migrate to NMCI and any reference to it will be removed from ISF Tools.

As part of the rationalization process, the following actions need to be accomplished:

- Derive raw application list from the ISF Tool database
- Categorize applications by type and functionality
  - o Apply NMCI Rulesets
  - o GOTS and COTS Rationalization
  - o Apply available standards
- Apply UTAM

4.3.1 Standardization and the Gold Disk

In order to reduce the number of applications within the enterprise, the DON has begun implementing standardization of applications. Since there are numerous applications that can perform the same function, the DON has begun selecting standard applications to be used across the enterprise. In this manner, applications that perform the same function are minimized to provide for a smaller list of Legacy Applications.

The first major step in standardization is the NMCI Standard Seat Service or Gold Disk (Appendix B). The DON has determined that all the NMCI desktops are to employ the applications contained in the Gold Disk. Further, per CNO Washington DC (N09T) message dated 120155Z JUN 02, the DON requires all Echelon II Commands to eliminate any unnecessarily duplicative application(s) from their rationalized list. If an Echelon II Commander requires an additional version of an application on the Gold Disk or other applications performing the same function, the Commander must request an exception from the Naval IO and the applicable FAM as outlined in the aforementioned message.

NOTE: The unique function being performed by the unique application and why it is operationally required needs to be included.

Similar to the Gold Disk, the DON has determined certain Legacy Applications that are standards. The latest list of standards can be found in the CNO Washington DC (N09T) message dated 120155Z JUN 02 (Appendix D). Each Echelon II Command is required to establish application version control following the Standardized COTs and GOTs applications list. Echelon II Commands need to update application versions on their rationalized list in the ISF Tools Database to reflect the versions listed in this message.

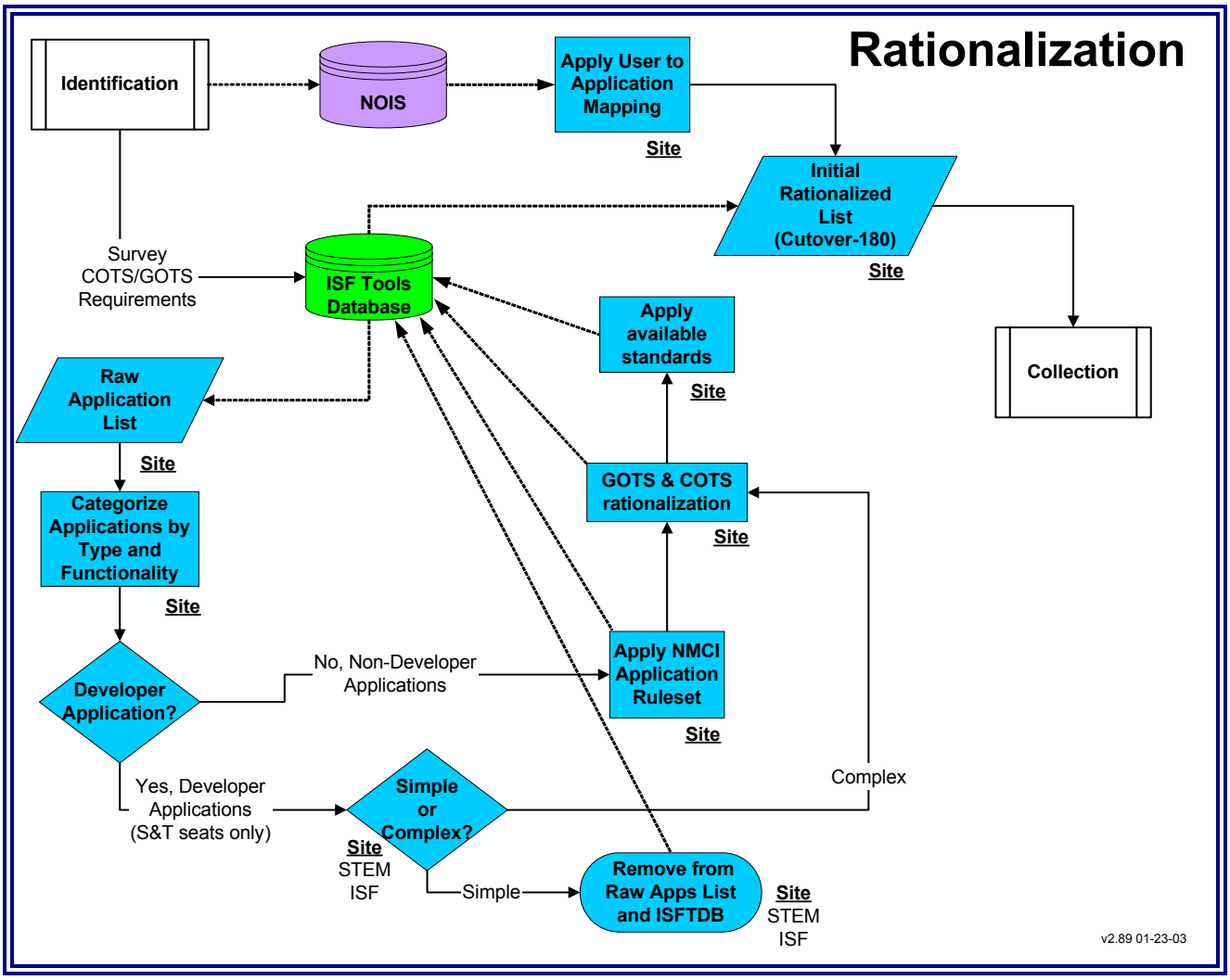


Figure 4-4. Rationalization

4.3.2 Derive Application List From the ISF Tool Database

Once the site has entered all Legacy Apps into the ISF Tools Database, a list of applications for that site can be created. This list and other information will be used in the Rationalization process.

4.3.3 Categorize Applications by Type and Functionality

Legacy Applications should be grouped and categorized by type and functionality. Grouping and categorizing is a useful tool in determining which applications are mission essential. For example, all of the graphics and design applications can be grouped into a category called “Graphics Design”. When all of these graphics and design applications are grouped they can be reviewed for overlap, redundancy, excess, and relevance. From this the Command/Site selects their rationalize applications.

4.3.4 Determine if Application is for Software Development

During this step, the Command/Site will determine if the application is used in the development of software applications. Software development tools can include functions such as database creation and administration, code generation, compliers and any other application for software development. This step is necessary because software development tools cannot be used on standard NMCI seats. Software development tools can only be used on NMCI Science and Technology Seats (S&T).

If the application is determined not to be a development tool, then other standards and rules will be applied to the application as part of the rationalization process.

4.3.4.1 Simple vs. Complex Developer Applications

Once the application has been categorized to be a development tool, then it must be determined if it is a simple or complex application.

A simple application is defined as a standalone application that requires installation on an NMCI workstation only, and has minimal to no dependency on network connectivity to function. The requirement for these applications to use the network for file share and network printer requirements does not make them complex. For example, most word processing applications are considered simple application.

Applications that require network connectivity for standard operation are, for the purposes of this program, defined as complex applications. Any applications that have a separate front end and back end, and require network connectivity to be fully functional, are considered complex. Server based and client/server applications are examples of complex applications. See the Section 4.3.4.2 below on this type of NMCI Seat.

If the software development application is categorized as simple it will be removed from the ISF Tools Database List and will undergo no further tracking/testing by the ISF. If the software development application is categorized as complex the ISF will require evaluation and testing to determine the application's impact on the network. Thus, it must be tracked in the ISF Tools Database and appear on the Command's/Site's Legacy Application Rationalize List.

4.3.4.2 Science and Technology (S&T) and Developer Seats

S&T or Developer Seats are designed for use by application developers, science and technology researchers, and anyone for whom a "locked-down" desktop will prohibit mission accomplishment. It is not intended for these seats to be purchased as work-arounds to the NMCI implemented desktop lockdown. These desktops can be requested under CLIN 38. S&T seats are minimally supported by the ISF due to the likelihood of user caused system failures. Customers who order these seats are responsible for maintaining desktop operation and functionality. The ISF will assist the S&T seat user if the seat needs to be re-imaged due to operating system failure or if the Gold Disk

applications need to be reinstalled. The ISF retains responsibility for non-developmental application support. Further, the ISF remains responsible for hardware support. Further, developer application support is available through CLIN 23 for S&T seat use only.

4.3.4.3 Apply NMCI Rulesets

Another important step in rationalization is applying the NMCI Ruleset to the Command/Site's list of applications. This list is maintained by the NADTF, a Navy CIO organization. Any applications that violate this Ruleset should be removed from any application list.

Note: The Ruleset pertains to applications, the ISF Tools Database and the Legacy Applications Rationalized List.

The NADTF will review all Rationalized Lists and will apply this Ruleset. Any applications that do not meet this Ruleset will be Killed by the NADTF and will not be permitted to reside within NMCI or within the quarantine boundary. Some rules are waiverable and requests for waivers for those applications will be submitted by the responsible Echelon II Command to the Navy IO Attn: NADTF. For the NADTF Waiver Process refer to Section 4.3.4.3.3 below.

The following rules apply to GOTS and COTS applications within NMCI:

1. Windows 2000 (W2K) Compatible
2. NMCI GPO Compatible
3. No Duplication of Gold Disk Software or Services
4. Comply with DON/NMCI B1 and B2 Policies
5. No Setup, Installation, Uninstallation, Update and Auto Update Tools or Utilities
6. No Games
7. No Freeware or Shareware
8. No Beta/Test Software (Authorized on S&T Seats Only)
9. No Application Development Software (Authorized for S&T Seats Only)
10. No Agent Software.
11. Gold Disk Compatible
12. No Peripherals, Peripheral Drivers or Internal Hardware in the ISF Tools Database or on the Rationalized List
13. No personal, non-mission, or non-business related software
14. No 8/16-Bit Applications

For a description and more details on the Ruleset, go to Appendix I, or to the NADTF website at http://cno-n6.hq.navy.mil/NaVCiO/leg_apps.htm

Additionally, sites are encouraged to consider IT for the 21st Century (IT-21) or Marine Corps Tactical Network (MCTN) published standards to aid in the decision. Plus, sites should consider the TFWeb initiative during the rationalization of the applications.

Other applicable rules may emerge from the DoD, DON, or the Echelon II Command. The rationalization is actually performed by a customer actively selecting an application via the ISF Tools Database. The output of this effort is the Initial Legacy Applications Rationalized List. Another output of the ISF Tools Database is the "site workbook." A listing of all of a site's Legacy Applications, a workbook shows certification status and other notes for each application as it moves through the transition process.

4.3.4.3.1 Killed Applications

The NADTF will Kill applications that violate the NMCI Ruleset. These are applications that are not compliant with the rules and standards for applications within NMCI as set by the Navy IO. These Killed applications will not be utilized in NMCI and **will not** be Quarantined. These applications will be removed from the Rationalization List and ISF Tools database, unless the rule is waiverable, a waiver to the rule is submitted, and the waiver is approved. Generally, NADTF will not consider waivers for these applications. However, if a site determines that a rejected application is mission-critical, a waiver can be sent following the guidelines of CNO message 252250Z FEB 02.

As a general rule, the FAMs and NADTF will Kill applications that do not have version numbers listed in the ISF Tools Database. It is up to the Command/Site to place the proper version number with the application listing in the ISF Tools Database. Once the Command updates the version number, NADTF will go back and updates the status to approve. Waivers must be submitted to the NADTF for those Killed applications that legitimately have version numbers.

4.3.4.3.2 Failed Applications

Fail is defined as an application that violates the NMCI Application Ruleset by failing to successfully meet compliance or usability testing standards. These applications are flagged as Quarantined and will operate on a Quarantined workstation in the legacy environment until the Ruleset violation or test failure is resolved or a waiver to operate within NMCI has been submitted and approved.

The ISF Tools Database and the Site's workbook will indicate the status of the failed application. The Failed Application will not transition into the NMCI environment until the problem is fixed. Once the problem has been resolved, the status will be changed in the ISF Tools Database

Table 4-1. Ruleset

Ruleset		Waiver ?	Quarantine ?
Rule 1	Windows 2000 (W2K) Compatible	NO	Yes – No More than 6 Months
Rule 2	NMCI Group Policy Object (GPO) Compatible	NO	Yes – No More than 6 Months
Rule 3	No Duplication of Gold Disk Software or Services	YES	NO
Rule 4	Comply with DON/NMCI Boundary 1 and 2 Policies	NO	Yes – No More than 6 Months
Rule 5	No Setup, Installation, Uninstallation, Update and Auto update Tools or Utilities	NO	NO
Rule 6	No Games	YES	NO
Rule 7	No Freeware or Shareware	NO – (Freeware) YES – (Shareware)	NO
Rule 8	No Beta/Test Software (Authorized on S&T Seats Only)	NO	NO
Rule 9	No Application Development Software (Authorized on S&T Seats Only)	NO	NO
Rule 10	No Agent Software	NO	NO
Rule 11	Gold Disk Compatible	NO	Yes – No More than 6 Months
Rule 12	No Peripherals, Peripheral Drivers or Internal Hardware	NO	NO
Rule 13	No personal, non-mission, or non-business related software	YES	NO
Rule 14	No 8/16-Bit Applications	YES	Yes – No More than 6 Months

4.3.4.3.3 NADTF Waiver Process

Waivers are required for:

- NADTF-Disapproved applications (Ruleset Failure)
- FAM-Disapproved applications (not part of the FAM portfolio)
- Waiver or quarantine application duration extensions

Waivers are not required for:

- Applications that are FAM and NADTF approved or not reviewed in ISF Tools
- Applications added to a Command's/Site's list in ISF Tools after Cutover minus 60 days that are FAM-approved and NADTF-approved or not reviewed
  - Processed as a MAC expense funded by the Command/Site
  - Installed after Cutover plus 30 days
- Applications that have not been reviewed by the FAM or NADTF

The NADTF has developed a NMCI Waiver Request Submission Guide to provide clear guidance for submitting NMCI Application/Change Waivers to NAVY IO (NADTF). Each Echelon II Command shall have a POC to manage the application and change process, and this includes the resources to submit and manage waivers for all subordinate Commands per the NAVY IO Guidance. One purpose of the LATG is to provide guidance in the proper rationalization of legacy applications to eliminate the need for a waiver. However, there may be a requirement for a waiver based on the status of the application being supported. It is critical that each Command/Site understand all requirements outlined in this guide and the references provided. Command/Sites must work with their assigned Echelon II POC to ensure all waiver requests contain complete and accurate information and are in the required format. The Waiver Input Template (WIT), as outlined in the link below, has been developed to improve accuracy and reduce duplication of effort on the part of the waiver requestor and the NAVY IO (NADTF).

The current version of the NMCI Waiver Request Submission Guide can be obtained through he NADTF website at: http://cno-n6.hq.navy.mil/navcio/file/nmci waiver submission guide_19 nov 2002.doc

The current status of waiver requests can be found on the NADTF Legacy Applications Home Page (http://cno-n6.hq.navy.mil/NaVCiO/leg_apps.htm)

4.3.4.4 GOTS and COTS Rationalization

The site will analyze the list of Legacy Applications for redundancy, functional overlap, and multiple versions of the same applications that are being used at the site. Duplicate and redundant applications will be eliminated prior to compiling the Rationalized List.

NOTE: If no owner for an application is identified, the application will not be allowed to migrate to NMCI and any reference to it will be removed from ISF Tools.

4.3.4.5 Apply Available Standards

Many Echelon II Commands/Sites have their own established software standards. If there are specific or other DON/DoD standards, they will be applied to the application list for processing.

4.3.4.6 Websites and URLs

Websites, especially those that download an application or portion of an application to the desktop, need to be identified so they can be tested by the ISF. These websites must be included in the rationalized list; otherwise, if not tested and approved, access to these websites cannot be guaranteed. The long-range plan for NMCI is to test, approve, and list in the ISF Tools Database the websites that the customers have requested. Then, sites will be able to select from a common list of websites that have been tested. If there is doubt whether a website falls into this category, place it on the Rationalized List and work with the ISF to verify it during testing.

4.3.4.7 Adding an Application to the Legacy Applications Rationalized List

An application must first reside in the Command/Site ISF Tools Database record. If selected from the Applications Catalog, it will appear on the Rationalized List. Legacy Applications that reside in the Command/Site database record that do not appear in the Application Catalog must receive approval for the appropriate FAM before it can be added to the Rationalized List. Once an application has been added to the Rationalized List, the Command/Site should submit a Command/Site/IG RFS to request access to the application at their Command/Site.

Legacy Applications that are not contained in the ISF Tools Application Catalog require FAM approval for entry into the ISF Tools Application Catalog.

4.3.5 Apply UTAM

This important transition step performed by the Command/Site is designed to ensure that applications selected for rationalization have a true user base. It is a useful tool in rationalizing applications. The Command/Site pulls the UTAM from the NOIS database and applies it against the Initial Rationalized List at Cutover -180. Applications that have no user base must be eliminated. Applications with a small user base must be closely evaluated for transition based on mission criticality.

4.4 COLLECTION

The Collection process is a Government responsibility. Figure 4-5 depicts the important elements of this step.

After the rationalized list is created using the ISF Tools Database, the Legacy Applications and supporting documentation must be collected for submission to the ISF Site Manager.

There are certain steps and procedures that need to be taken within the Collection process. These processes will occur concurrently:

- Associate to a Certified Application
- Identify Licenses
- Identify Desktop and Server connectivity (Network Diagram)
- Perform Final User/Application/Machine/Server/Peripheral Mapping
- Finalize Site Loadsets
- Generate and Gather IA Documentation and Items

4.4.1 Request for Service (RFS)

A RFS is a request by the transitioning activity to use a specific application in NMCI. All applications to be used at that activity require an RFS submission. The RFS is accessed and submitted electronically through the ISF Tools DB. There are two types of RFS submissions, a CDA RFS and a Command/Site/Implementation Group RFS.

4.4.1.1 CDA RFS

A CDA RFS indicates the version of the software that is most recent and fully supported by the owning CDA. The CDA version is always the preferred version of the application. The Command/Site should research the ISF Tools Application Catalog for an existing CDA RFS. If a CDA RFS does not exist for the requested application, one needs to be submitted. Only the CDA of the application can submit a CDA RFS. When a CDA RFS is submitted, the following items need to be collected to meet the media submission requirements:

- Installation Instructions and Test Scripts/Plans (See Appendix G for examples)
- Media and License Validation
- Network Diagram (desktop-to-server connectivity)

Further details regarding CDA RFS submissions can be found in the NMCI Release Development and Deployment Guide (NRDDG) (published separately).

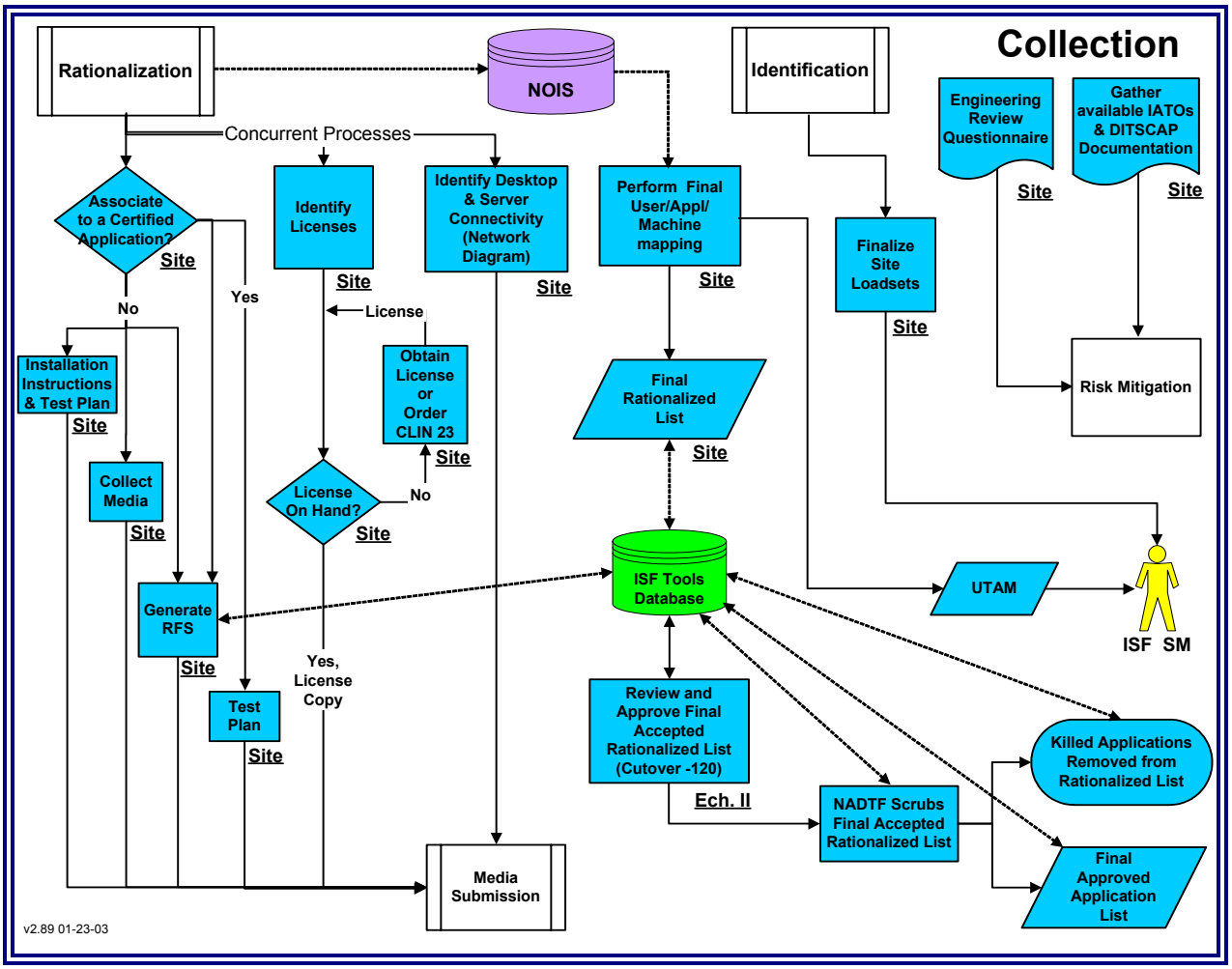


Figure 4-5. Collection

4.4.1.2 Command/Site/IG RFS

The Command/Site/IG RFS is for all those applications that do not have a CDA in support of the application. Navy IO policy requires all applications to have ownership. If a formal POR or CDA is not assigned to the application, by default, the Echelon II Command of the Command/Site requesting the application is the application owner. The Command/Site/IG RFS is used to gain access to the identified application at the NMCI Seat level.

Commands can exist at multiple geographic locations. Commands can have subordinate activities that exist at different geographic locations. ISF Tools uses Implementation Groups for defining all those geographic locations. Each subordinate activity or Command located at a specific geographic location (Site) is assigned to an Implementation Group, which represents their physical location.

Commands creating Rationalized Lists in ISF Tools may opt to create a Centralized Rationalized List. One instance for generating a Centralized Rationalized List is to allow a Command that exists in multiple geographic locations to utilize a single Rationalized List. Another instance for generating a Centralized Rationalized List is to allow multiple subordinate activities existing under the same Command to utilize a single Rationalized List. In either instance, a Command level RFS can be submitted for each application contained within the Centralized Rationalized List.

A subordinate activity or Command located at a specific geographic location (Site) may need to define unique characteristic information (i.e. configuration parameters, hardware constraints, etc…) about an application they require. In this case, a Site (Implementation Group) RFS can be generated in addition to a Command Level RFS to address those particular issues. When an Implementation Group RFS has been submitted, it only supersedes a Command Level RFS for the effected subordinate activity or Command identified at that specific geographic location.

Commands may allow subordinate activity(s) to create their own separate Individual Rationalized List. If the Command resides at a single geographic location and the rationalized list represents that individual Command, submitting either a Command Level RFS or an Implementation Group RFS achieves the same goal because the RFS submitted will only affect a single activity.

4.4.2 Identify Licenses

Commands/Sites must comply with all legal copyright rules regulations and laws. Government Agencies may require proof of compliancy with copyright laws at any time. However, for transition purposes, the ISF does not require verification of compliancy with copyright laws. The ISF does require proof of licensing for the copy of the application that is being submitted for NMCI Certification Testing. If a license is not available, proof must be obtained through an approved vendor, government agent or ordered through CLIN 23.

4.4.3 Identify Desktop and Server Connectivity (Network Diagram)

It is the responsibility of the Command/Site to provide, to the ISF Site Manager, the desktop and server connectivity in a Network Diagram. (Appendix G.6)

4.4.4 Perform Final User/Application/Machine Mapping

The Command/Site performs the final UTAM in NOIS, tying the users listed for seat orders with the applications identified in the ISF Tools Database. The Final UTAM is then turned over to the ISF SM. This step is to be completed 120 days before cutover. The Final UTAM should be used in the verification of the Final Rationalized List. It is understood that the UTAM will change between submission and cutover. The Command/Site will have additional opportunities to update the UTAM prior to cutover.

4.4.4.1 Create the Final Rationalized List

The Command/Site will perform a final review of the applications entered in the ISF Tools Database Application List. A final User-to-Application and User-to-Machine mapping is applied against this list for the final steps of rationalization. Once the final review is complete, the Final Rationalized List is forwarded to the appropriate Echelon II Command for review and approval.

4.4.4.2 Review and Approve Final Accepted Rationalized List

The Echelon II Command reviews and approves the Final Rationalized List. This approval is required for the list to be formally accepted. This review and approval produces the Final Accepted Rationalized List.

4.4.4.3 NADTF Scrubs Final Accepted Rationalized List

NADTF personnel will scrub the Final Accepted Rationalized List.

- Apply the NMCI Ruleset.
- Check the existing DON Standard Applications List.
- Check if the application is already certified and performing the same function.
- Check to ensure the version number of the application is the latest available.
- Verify the Command/Site's Unit Identification Code (UIC) .
- Verify that a CDA is assigned along with a previously submitted CDA RFS.

The NADTF will Kill applications not passing the criteria. Once finished, NADTF will approve the Command's/Site's Final Accepted Rationalized List, producing the Final Accepted Applications List.

4.4.5 Engineering Review Questionnaire (ERQ)

The ERQ is a document designed to collect all information pertaining to an application. The ERQ is used to analyze a system's requirements and configuration. This information is critical to the post-transition Accreditation procedures for the development of DITSCAP documentation and the Systems Security Authorization Agreement (SSAA). The ERQ is a prerequisite to begin the Risk Mitigation Phase. While not required during the Rapid Certification Phase, the ERQ information is most readily available as part of the Collection process of the Rapid Certification Phase. The ERQ template can be found at www.nmci-isf.com.

4.4.6 Gather Available IATOs and DITSCAP Documentation

If any prior Interim Authority to Operate (IATO) or DoD Information Technology Security Certification and Accreditation Process (DITSCAP) information exists for a legacy application being submitted, it should be collected and stored for use in the Risk

Mitigation Phase. If this information does not exist, the application owner will need to fulfill this requirement before the application can be fully Accredited in the Risk Mitigation Phase.

4.5 MEDIA SUBMISSION

Figure 4-6 depicts the steps for media submission. This process is primarily a Government responsibility, but there are several aspects of the process that are joint or ISF-only responsibilities. Refer to the NMCI Legacy Applications Submission Guide found on the NMCI web page at www.nmci-isf.com/downloads/NMCILegacyAppSubmitGuide.doc The NMCI Legacy Applications Submission Guide details the procedures and documents needed for submission of media and documentation to the ISF.

After an application's media and support materials are collected, they must be submitted to the ISF to begin the NMCI Certification process. As mentioned in the Collection process description (Section 4.4) there are two types of submissions: Legacy Applications submitted through the CBA process and new Legacy Applications.

All Legacy Application media and materials will be submitted to the ISF Site Manager (SM). If the ISF SM has not arrived on site, the Command will hold all materials until the SM arrives.

4.5.1 Initial Assessment and Testing Decision

The Command/Site will turn the submission over to the ISF SM. The ISF and STEM teams will perform an Initial Assessment of the submission, which includes a Completeness Review and a determination of where the application will be processed for certification.

The ISF and STEM teams will perform the Completeness Review. If any parts of the required submission are missing or incomplete, the STEM team will work with the Command/Site to provide them. If the submission passes the completeness review, the Legacy Application type is determined:

- CBA Legacy Applications (with their RFS) will be examined and retained on-site for processing.
- New Applications (non-CBA applications) will be reviewed to determine the Certification process. The ISF will decide to either:
  - Retain it on-site for Local Deployment.
  - Send it to the San Diego AIT Lab for Packaging and Certification.
- Copies of all network diagrams and other documentation are retained by the ISF.

Note: Certification process and location is an ISF decision.

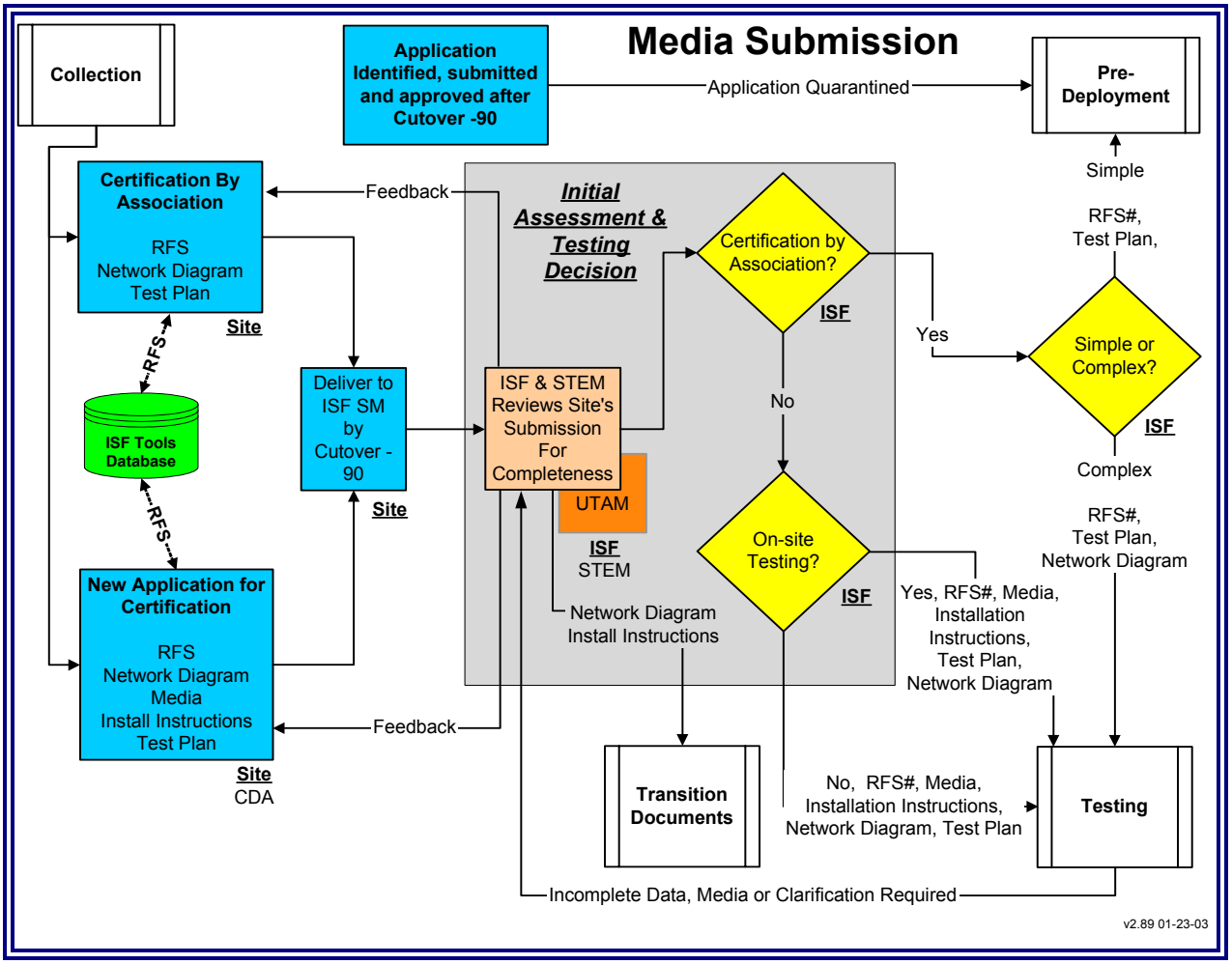


Figure 4-6. Media Submission

4.5.2 Submission Deadlines

All application submissions are due to the ISF SM by Cutover -90 days. Customers must submit their media and supporting documentation on time. The ISF must have time to process (Certify) the application for transition. Missing this deadline will cause those applications to be late. Any applications submitted late are subject to the Late Identification and Submission Process. (See Appendix C).

If the media and supporting documentation are not submitted by Cutover, the application will be considered an "emergent" requirement and not considered to be a Legacy Application based on the NMCI contract terms. The Command/Site and /or the Echelon II Command will be responsible for the financial implications associated with the NMCI Certification and transition of these applications.

4.6 TESTING

Testing consists of two processes, AIT Lab Testing and On Site Testing as depicted in Figure 4-7. Lab Packaging, Certification and Testing are done only at the AIT Labs in San Diego. On-site Packaging and Testing are done via the PIAB and LDSD&T tests at site. Applications are never Certified on-site. The Testing processes are discussed below.

During the testing process the application status is recorded and tracked in the ISF Tools Database. AIT Lab personnel and SSE teams will record the status of the various steps within the process using this tool.

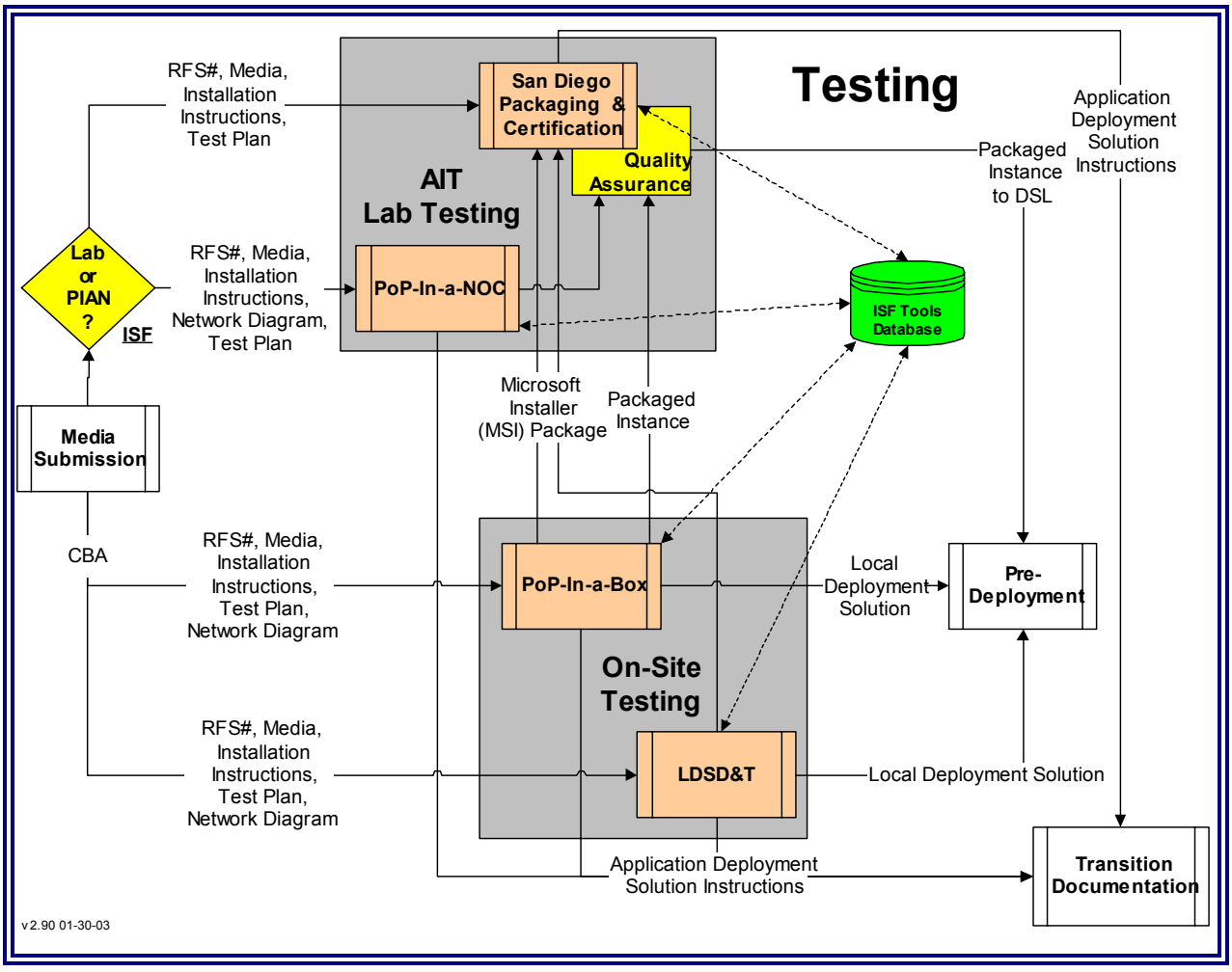


Figure 4-7. Testing

4.6.1 Local Deployment vs. Push

Several criteria are used to determine how an application is handled and processed. User base and Enterprise impact are major criteria used to determine the process an application will go through. Applications that have an overall Enterprise appearance and a high user base are likely to be processed through the San Diego AIT Lab to create a packaged Enterprise solution that can be centrally managed. Large Enterprise (CDA) applications are prime candidates for central packaging and push. Those applications with a low user base and local impact only are good candidates for the On-Site Testing Processes and Local Deployed. The UTAM is one of the main tools used to determine an application's user base.

NOTE: The ISF has the responsibility to determine the most effective way to deploy a Legacy Application, and they will route the Legacy Application to the appropriate testing location and method.

A Local Deployed application is one that does not utilize the packaging and push processes. Local Deployed applications are placed on the NMCI desktop through means other than the Novadigm Radia push (explained below). There are many ways the application can be loaded to the desktop; examples include: manual hand load, central server load, and File Transfer Protocol (FTP) download, etc.

NOTE: The ISF will determine the most efficient process to Local Deploy an application**.**

When an application has an enterprise exposure and a high user base, locally deploying that application is not practical. Therefore, creating a centrally managed enterprise solution is usually the best option. An application is "pushed" through an automated process that originates at the San Diego AIT Lab and runs through a set of software servers from the NOC through the server farm to the site. This "push" process is accomplished, managed, and distributed using the Novadigm Radia tool and active directory. In order for an application to be automatically delivered (pushed) to the desktop, the application must be packaged for delivery. Applications that are packaged and pushed using Novadigm Radia take advantage of centralized software management that delivers applications to the desktop without the user going through an "install" process.

4.6.2 San Diego Packaging & Certification

Figure 4-8 depicts the process of San Diego Packaging & Certification. Those applications selected for San Diego Packaging and Certification are sent to the San Diego AIT Lab by the ISF site personnel. CDAs should submit their versions directly to the San Diego AIT Lab after making the appropriate entries in the ISF Tools DB and creating a CDA RFS.

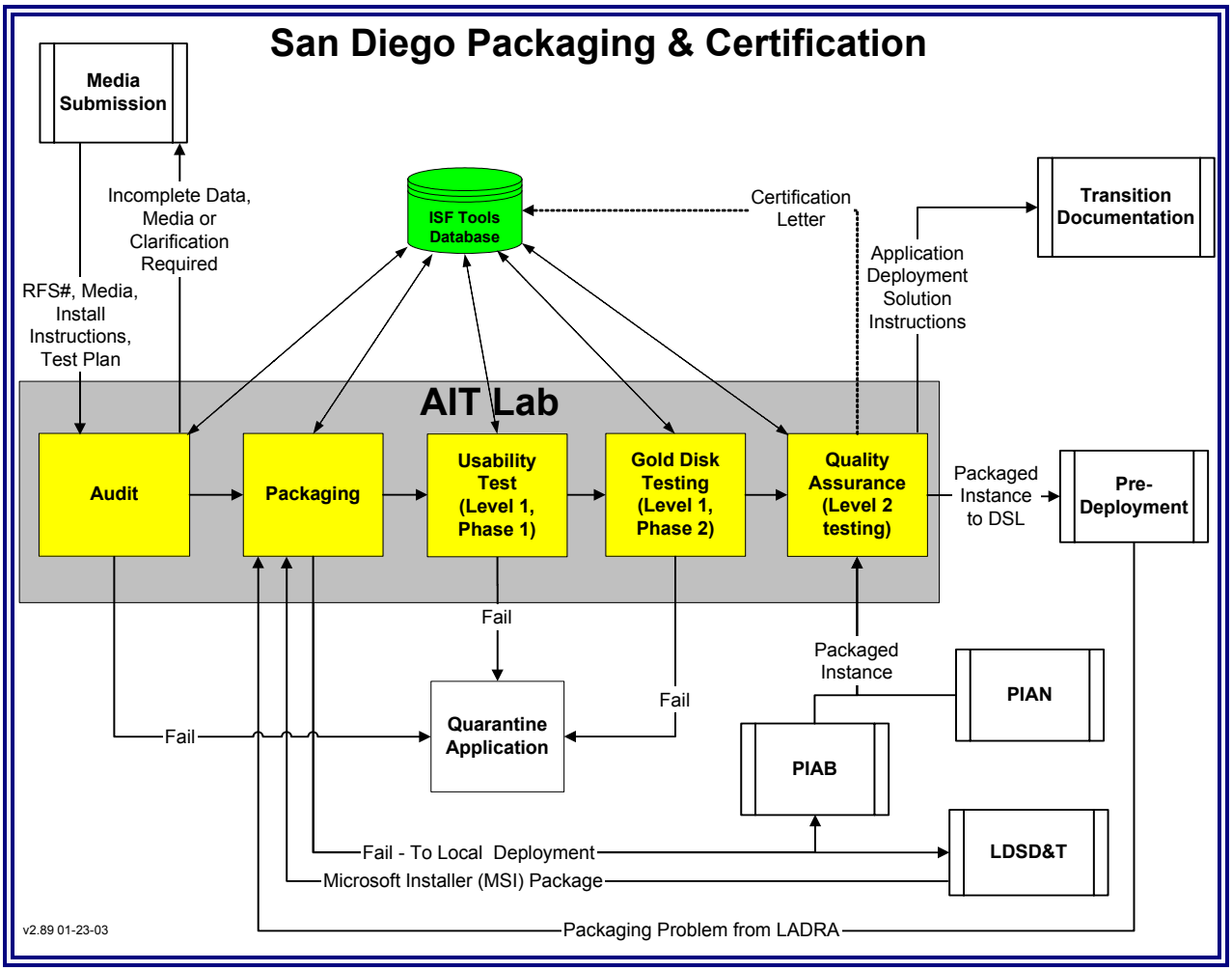


Figure 4-8. San Diego Packaging and Certification

Once received in the lab, applications are processed through Packaging Audit, by the ISF lab personnel to verify that the media submitted is valid and there are no viruses. Any installation instructions are reviewed for completeness, along with all other needed documents and information.

The AIT or EAGLE Team personnel notify the Command/Site/CDA of problems with any submissions. The ISF Tools Database is updated by AIT Personnel to track the status of the application during testing, certification and packaging.

After a successful audit, the application is packaged using Novadigm Radia, then goes through the Lab Usability Test (Level 1 Phase 1). If the application fails to package, the application will be returned to the Command/Site for Local Deployment processing or the CDA for remediation. If the application successfully packages, it is then run through the Lab Usability Test.

The Lab Usability Test determines if the "Package" executes successfully and the application runs properly in the Windows 2000 environment. It does not test end-to-end connectivity, run a trace, nor involve "users". Failure of the Usability Test will send an application to Quarantine. Next, the GPO Ruleset in the Enterprise GPO established by the Navy and ISF is applied. An application's failure to operate with the Enterprise GPO will cause that application to fail and be Quarantined.

Upon completing the Lab Usability Testing, the application is tested against the Gold Disk of standard NMCI applications for interoperability issues. Failure of the Gold Disk Test will send an application to Quarantine.

Any configuration notes recorded as part of the packaging and testing process are stored as transition documentation.

When an application has completed the Certification Process at the San Diego AIT Lab and NMCI Certification has been granted, the NMCI Certification Letter is created in the ISF Tools Database. A copy of the Certified Radia Instance is stored at the Definitive Software Library (DSL).

Some applications will require on-site testing to make sure that they function properly for the site. These applications will undergo a Usability Test on site or in the PIAN.

For those Legacy Applications that are to be CBA to an already NMCI Certified application, many of the early steps in the process are skipped, including the Radia packaging. The Radia instance of an application that is already in existence is used for this CBA situation. These applications are already packaged, so they can immediately proceed to the on-site Usability Test sub-process as detailed in Section 4.6.5 of this guide.

If an application fails during the Packaging portion of the process, it will be referred back to the site for processing as a Local Deployment application. A package can fail the Packaging process if the media is not valid, installation instructions are incomplete or other issues are found with the packaging.

Note: During the Packaging and Certification process, the status of the various steps is recorded and tracked in the ISF Tools Database by AIT Lab personnel.

4.6.3 Pop-In-A-NOC (PIAN)

Figure 4-9 depicts the PIAN process. The PIAN is primarily a post transition tool for use by CDAs for introducing applications or changes into the NMCI environment. The primary function of the PIAN is to test priority applications that need outside connectivity to a server as identified by SPAWAR code PMW164. However, the ISF may also use the PIAN to create a deployable packaged instance for CDA applications.

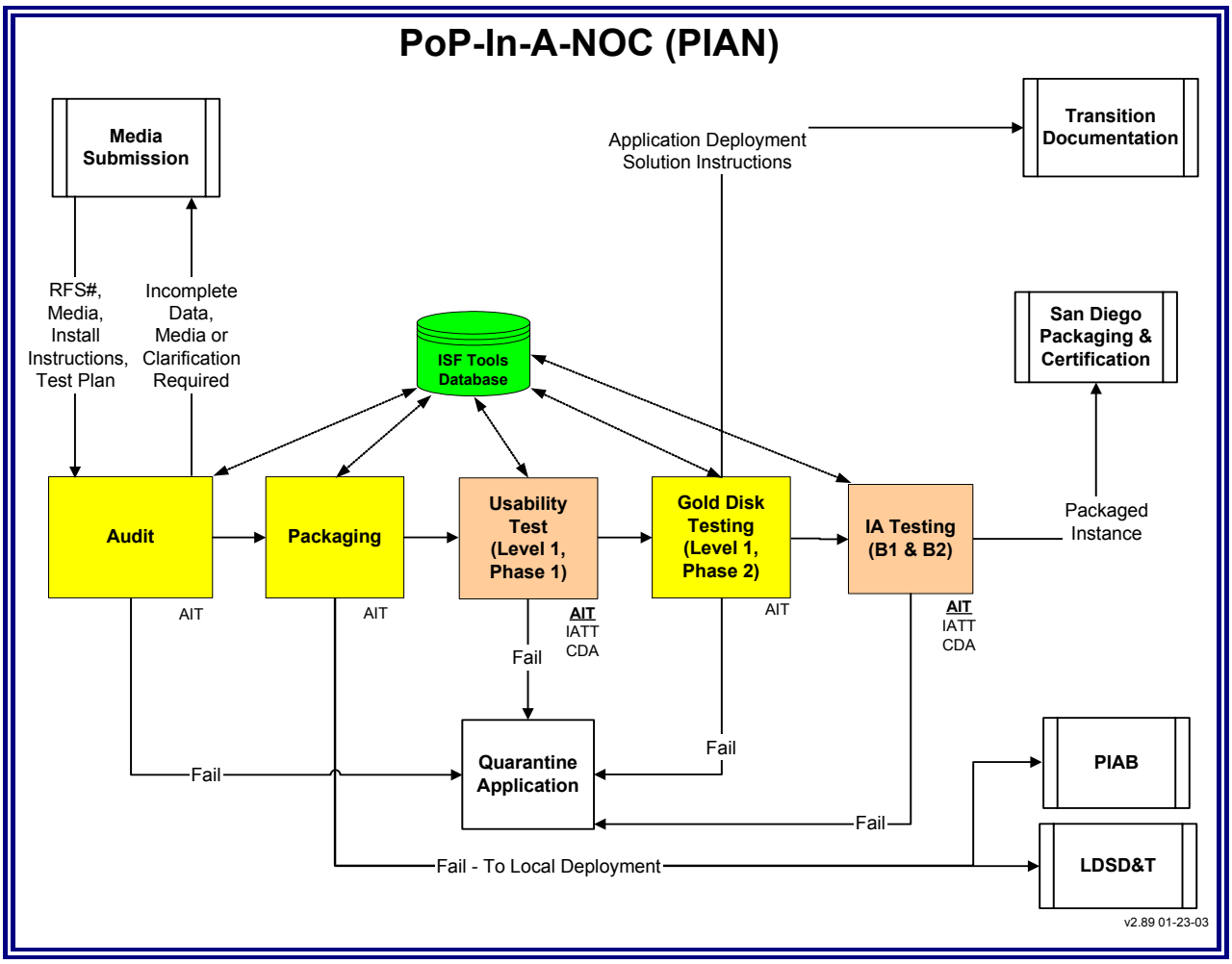


Figure 4-9. PoP-In-A-NOC (PIAN)

Further, the ISF can use the PIAN to process transitioning legacy applications to determine solutions.

Those applications selected for PIAN are handled like any other application destined for the AIT Lab in San Diego. Once in the lab the ISF will determine if it is best to process the application through the PIAN.

NOTE: It is the ISF decision to utilize the PIAN to process the application. The Command/Site/CDA may provide input into this decision.

Once in the PIAN applications are run through a Packaging Audit by AIT personnel to verify that the media submitted is valid and there are no viruses. Any installation instructions and other needed documentation are reviewed for completeness. AIT or EAGLE Team personnel notify the Command/Site/CDA of problems with any

submissions. AIT personnel to track the status of the application during testing, certification and packaging update the ISF Tools Database.

If an application testing issue arises such as incomplete data or bad media, or if clarification is required, the AIT personnel will work with the EAGLE Team and/or the CDA to correct any issues so that testing can be completed in a timely manner. If during the Audit the application is found to be non-deployable within NMCI, the application will be Quarantined. For the reasons why an application may fail Audit please see the NMCI Ruleset found in Appendix E.

Next, the applications are "packaged" into an electronically deployable "instance" using special software called Novadigm Radia. These "instances" allow the application to be centrally deployed and managed using Active Directory. If the application cannot be packaged or has failed the NMCI Ruleset, then the application will be sent for local deployment testing either with PIAB or LDSD&T.

Once successfully packaged, the application is run through the PIAN Lab Usability Test (called Level 1, Phase 1 and 2 Testing). The Lab Usability Test differs from the site Usability Test. Though both tests have commons steps, the Lab Usability Test does not test end-to-end connectivity, run a trace, nor involve "users". Its primary purpose is to determine if the "Packaged Instance" of the application executes successfully and that the application runs properly in the Windows 2000 environment. Failure of the PIAN Lab Usability Test will cause an application to be Quarantined.

As part of the Lab Usability Testing, the application is tested against the Gold Disk of standard NMCI applications for interoperability (Level 1 Phase 2 Testing). Failure to successfully interoperate with the NMCI Gold Disk will result in an application being Quarantined.

Finally, IA testing and processing is performed. These steps test the application for compliance with the IA policies, rules, settings and infrastructure. Failure of IA testing will lead to the application being Quarantined. The data captured during the IA testing is used during the Risk Mitigation Phase for Accreditation leading to the DITSCAP documentation and the SSAA.

Following successful completion of the IA testing, the packaged application instance proceeds to the San Diego AIT Lab for the Quality Assurance (Level 2) testing step. This is essentially a quality control check of the application's packaged instance. After successful completion of this final test, the packaged instance is sent to the DSL for push to the network and seat.

Note: During the PIAN processes the status of the various steps is recorded and tracked in the ISF Tools Database by AIT personnel.

4.6.4 On-Site Testing

Applications retained on-site for Local Testing can be tested using one of two tools available to the ISF SSE Team: the PoP-In-A-Box (PIAB) or the NMCI Test Seat used in the Local Deployment Solution Development and Testing (LDSD&T) process.

To begin any On-Site Testing, the applications are evaluated for their suitability for packaging and push to the desktop. Applications selected for local packaging will be processed by the ISF SSE team via the PIAB (if there is a PIAB on site). If there is no PIAB at the site, the application cannot be packaged for push. If the application is unsuitable for packaging, it can be processed through the PIAB or LDSD&T for a Local Deployment solution.

4.6.5 PoP-In-A-Box (PIAB)

Applications start with an Audit by the ISF SSE team to verify that the media submitted is valid and there are no viruses. Any installation instructions are reviewed for completeness. Problems with any submissions are turned over to the STEM for resolution with the site. Figure 4-10 depicts the PIAB process.

The SSE Team then determines how they will deploy this application. Their choices are Package and Push or Local Deployment.

4.6.5.1 PIAB Package and Push

The Packaging and Certification procedures performed on-site or in San Diego AIT Lab are almost identical. The application is "packaged" into an "instance" using special software called Novadigm Radia. Once the application has been successfully packaged, the application instance and all supporting documentation are sent for local usability testing. Applications that fail to successfully package will be sent to Prepare Local Deployment Solution to be processed as a local deployed application.

4.6.5.2 PIAB Local Deployment

Local Deployment applications and all supporting documentation are sent for Local Usability Testing. Applications that fail Local Usability Testing will be Quarantined. After the Usability Testing, the application is tested against the Gold Disk of standard NMCI applications to look for interoperability issues. Failure to interoperate with the Gold Disk will cause an application to be Quarantined.

Applications that successfully pass all steps of the PIAB are ready for final Legacy Application Deployment Readiness Activity (LADRA) testing and deployment. Local Deployment applications are retained on-site for deployment. On-site packaged and tested applications are copied and sent to the San Diego AIT Lab ("Packaged Radia Instance" is another name for the packaged application) for the Final Certification Lab Process and load to the DSL servers.

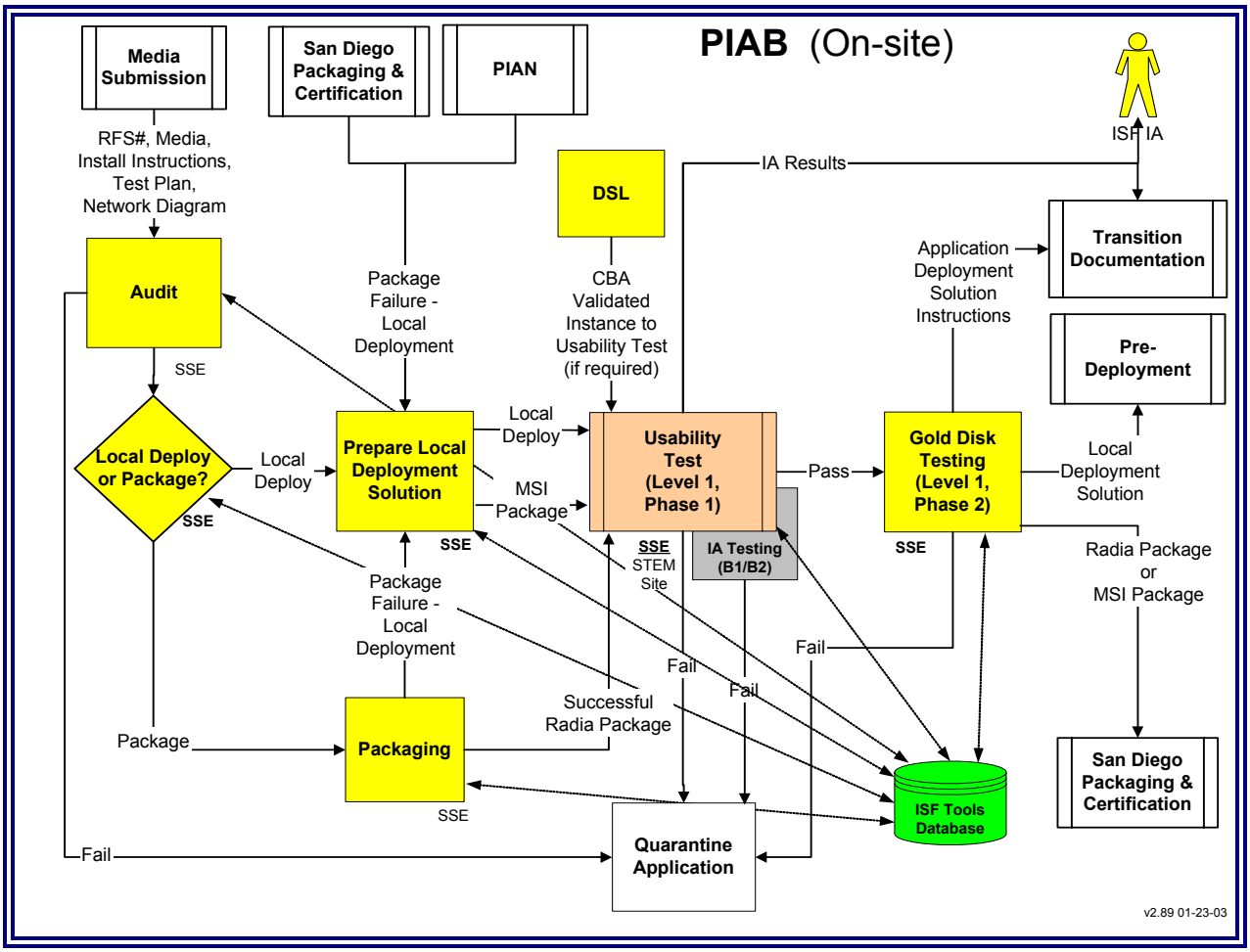


Figure 4-10. PoP-In-A-Box (PIAB)

NOTE: During the PIAB process, the testing and certification status is recorded and tracked in the ISF Tools Database by the SSE team.

4.6.6 Local Deployment Solution Development and Testing (LDSD&T)

The LDSD&T process is depicted on Figure 4-11.

LDSD&T is used when local testing is warranted and a PIAB is not available. LDSD&T requires the NMCI Base Infrastructure to be installed and active, but does not require connection to the live NIPRNET environment. The ISF uses standard NMCI Seats installed on the Base Infrastructure to perform the application testing and processing. These standard NMCI Seats have special software installed and are called NMCI Test Seats.

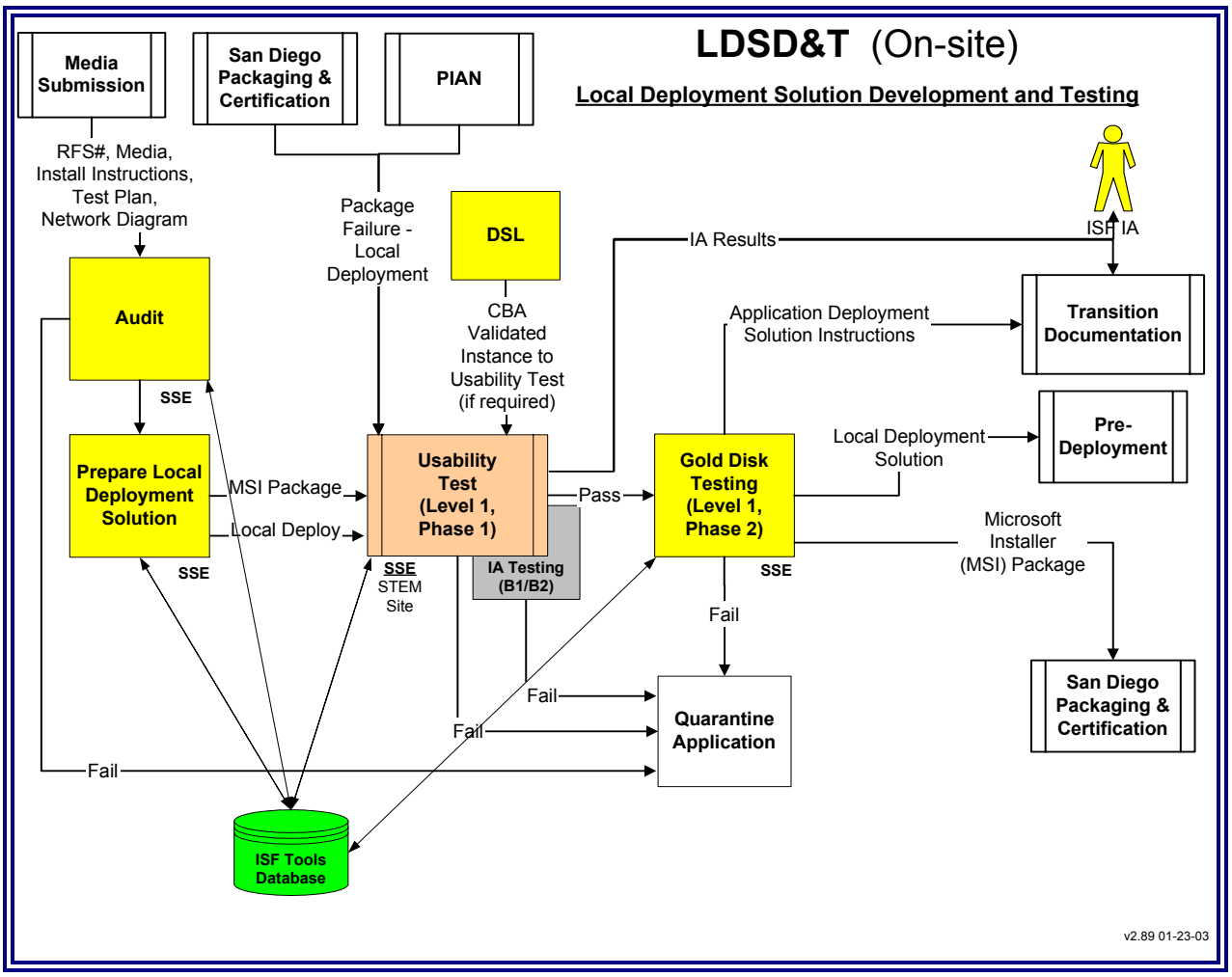


Figure 4-11. Local Deployment Solution Development and Testing

The LDSD&T process starts like all other testing processes with an Audit of the submission. Applications start with an Audit by the ISF SSE team to verify that the media submitted is valid and there are no viruses. Any installation instructions are reviewed for completeness. Problems with any submissions are turned over to the STEM for resolution with the site.

Applications are then sent to Usability Testing. CBA Legacy Applications are sent to Usability Testing to be tested for local use. Applications that fail Local Usability Testing will be sent Quarantined.

After the Usability Testing, the application is tested against the Gold Disk of standard NMCI applications to look for interoperability issues. Failure to interoperate with the Gold Disk will cause an application to be Quarantined.

All applications that are processed as part of LDSD&T will also proceed through the Legacy Application Deployment Readiness Activity (LADRA) testing (as described later

in this guide). Often the SSE team will combine the LDSD&T and LADRA testing into one seamless procedure.

NOTE: During the LDSD&T process, the status of the various testing steps is recorded and tracked in the ISF Tools Database by the SSE team.

4.7 USABILITY TEST

The Usability Test is a sub-process of the Certification process and used in the on-site testing processes. ISF has primary responsibility for this step, but the government can be involved in the joint process.

The Usability Test is conducted on-site with either PIAB or an NMCI Test Seat. The PIAB test environment simulates the NMCI environment and allows a network trace to be performed when the application is active. The NMCI Test Seat is an actual NMCI production desktop with special configurations and software for testing the application and running traces. The PIAB is used when the NMCI base infrastructure is not complete. Once the base infrastructure is in place, NMCI Test Seats are utilized to complete application processing.

This sub-process starts using the following applications:

- Newly packaged on-site.
- On-site certified application that will be locally deployed.
- An already packaged NMCI Certified Radia Instance that has been sent to the site from the San Diego AIT Lab.

The packaged application is pushed to, or the local deployed application is deployed to, a "test cell" in the PIAB or NMCI Test Seat. For an application that will use CBA, the ISF can gain access to this previously certified application by downloading it via the on-site FTP server. This application is then deployed to the test seats for processing.

If there are any special configuration changes needed to get the application to install properly, that configuration information is documented as an Application Deployment Solution (ADS) Instruction. The Command/Site user/application owner/CDA will assist with any configuration changes.

After the application has been configured, actual users are brought to the PIAB/NMCI Test Seat as part of Usability Testing. Commands/Sites are responsible for identifying and scheduling a designated user/tester. A designated user/tester should be selected who is familiar with the installation and usage of the application. The designated user/tester must come to the testing area ready to process the application from end-to-end when scheduled. To ensure proper support during application testing, Commands/Sites should designate a primary and alternate user/tester for every application.

Note: Commands/Sites are responsible for identifying and scheduling a designated user/tester.

If the designated user/tester is not available to test the application, that application cannot be tested. The STEM and ISF SSE team, in coordination with the Command/Site and SIL, will attempt to contact and schedule the user/tester twice. If, after two attempts, the user/tester cannot be scheduled or fails to support the application processing/testing, the application will be set-aside for Quarantine. Processing an application Quarantined for lack of user support will be done when ISF resources are available as long as it does not delay Cutover.

The user portion of Usability Testing is accomplished using a test script (if one has been provided) or free form by the user/tester. An example of a Test Script can be found at Appendix G.4. In addition, while the testing is being done the SSE team will run the network trace using a sniffer test (EtherPeek software) to trace the ports, protocols, and services used by the application. The results of the application test will be documented by the SSE Team and sent to ISF IA personnel. Each application is also reviewed for compliance with B1 and B2 firewall policies. For more information on NMCI IA and Boundary Definitions, the reader is referred to the NMCI Contract and Appendix H. The PIAB/NMCI Test Seat results (which include the network trace) and other information are used during the Risk Mitigation Phase.

The Packager/Certifier will analyze the configuration changes that were needed to allow the application to install and run properly. If needed, the application will be repackaged with the new configuration information. Any configuration changes that cannot be included in the packaged application are noted so that they can be performed as part of the desktop deployment. The repackaged application will be pushed to a test cell in the PIAB or NMCI Test Seat. It will be analyzed to verify that the repackaged application is working properly and no further configuration changes are needed.

As the final step, the Packager/Certifier will prepare the packaged application for the Gold Disk testing.

Note: If an application fails any part of the Usability Test (non-Win 2K compliant, poor interoperability, non-GPO compliance, non-B1/B2 compliance, etc.) it will be Quarantined. After the initial seat Cutover, this application and its solution must be re-evaluated for a final disposition.

4.7.1 Transition Documentation

The Transition Documentation process is an ISF responsibility, but is described here for informational purposes.

Application information for a site is stored in the Site Folder (a collection of documents kept on-site for immediate and future reference), the Application Document Storage site (an electronic storage site used by the ISF), and the ISF Tools Database.

These various information storage locations help the ISF complete their job and assist in the creation of the Applications Deployment Solution Instructions. These documents detail the connectivity solution for each application at a specific site. This information will be used in the Risk Mitigation Phase of the site's NMCI transition.

4.7.2 Information Assurance (IA)

NMCI security and IA are critical to the success of NMCI. Through layers of technical protections and procedures, NMCI enables its users to access information and services with the trust necessary to do their jobs. Defense-in-depth protection mechanisms are deployed in a layered fashion forming boundaries at multiple levels within the security architecture. This process ensures resistance to attacks and minimizes the possibility of a security breach due to a weakness (known or unknown) at any single security component. The defense-in-depth protection strategy provides security features to NMCI systems and data. These features are confidentiality, integrity, availability, accountability, and non-repudiation. Elements comprising various aspects of IA provide those security features.

IA consists of two parts: policy and implementation. Policy is a government responsibility, while implementation has been delegated to the ISF. The NMCI DAA sets the policy for the Enterprise B2 and the GPO, which has also been referred to as Boundary 4. The Enterprise B1 policy is known as the Navy Marine Corps Enclave Protection Policy (NMCEPP) and is set by OPNAV/CNO. For more information regarding boundaries, refer to Appendix H. ISF is responsible for the implementation of the Boundary and GPO policies set by the NMCI DAA and OPNAV/CNO. The implementation of the policies is accomplished in two phases, the Rapid Certification Phase and the Risk Mitigation Phase.

During the Rapid Certification Phase, the overall goal and end state is seat migration. This means the NMCI desktops are operational and can function in the NMCI environment. Before the seats can be migrated, the Enterprise B1, B2, and GPO policies are implemented. IA data is collected on the applications, but is not analyzed. This data will be used in the Risk Mitigation Phase. NMCI DAA has Authorized access to Legacy Applications using a type accredited Boundary 2. The NMCI DAA reviews the weekly report submitted by the ISF to ensure compliance.

IA Testing occurs during the Usability Test. PIAB and NMCI Test Seats are used to test the B1, B2, and GPO compliance. The application is loaded onto the NMCI test seat (either PIAB or LADRA). If the application is tested using a NMCI Test Seat and then functions properly, it is compliant with B1 and B2 firewall policies. If the application is tested using a PIAB, port and protocol data will be reviewed for compliance with the policies. All port and protocol data is passed on to the Risk Mitigation Phase. To test GPO compliance, the application is loaded on a test seat and if it functions properly, it is compliant with GPO. For more information on GPOs and examples of those that will be used in NMCI refer to Appendix H.

As mentioned in the Usability Testing section, any application that fails IA compliance testing will be Quarantined. A team of ISF and IATT members will review the application and make recommendations for modification during the Risk Mitigation Phase. Once the proper modifications are made, the NMCI DAA will grant an IATO/Authority to Operate (ATO) and the application will be allowed to migrate to the NMCI environment.

4.7.3 Enterprise B1, B2, and GPO Operational Management

Appendix H gives an overview of the IA Operational Management and NMCI Architecture. The appendix shows where B1 and B2 are implemented. Each boundary serves a purpose. The B1 (NOC) protects access to NIPRNet and Internet. The B2 performs similar functions as B1, except that the rules are more permissive for an interface with existing internal Navy and USMC networks.

4.7.4 Risk Mitigation

The Risk Mitigation Phase is a joint process between the Navy and the ISF, with the Navy's primary responsibility being IA policy and the ISF's responsibility being implementation. The overall goal and end state is server and system migration to NMCI. Risk and vulnerability reviews for the Legacy Applications will be conducted resulting in Accreditation for the applications. The IATO or ATO is needed to accomplish server and system migration in the Risk Mitigation Phase. In this phase, the Enterprise policies may be modified as necessary to reach migration. NMCI DAA approval is required to transition an application to the NMCI enclave.

Note: The Risk Mitigation Phase is beyond the scope of this guide.

4.8 PRE-DEPLOYMENT

The Pre-Deployment process is primarily an ISF responsibility. In this stage, the final preparations are made before actual delivery of user seats. Figure 4-12 shows the Pre-Deployment process.

There are several milestones in the Pre-Deployment process that must be met before the Legacy Applications Deployment Readiness Activity (LADRA) can commence:

- The Enterprise B1 is in place at the NOC.
- The Enterprise B2 and GPO are deployed.
- The Application Deployment Solution Instructions are ready.
- The local load applications are ready.
- The NOC is ready to "push" applications to seats. In order to accomplish this, the Radia Instances must be loaded from the DSL to the San Diego NOC and

uploaded to the designated NOC for deployment of the Legacy Applications to the site. For the deployment to the seat to occur, the Transition Team must create the User Profiles in the Active Directory. The Transition Team uses the UTAM and creates User Profiles in the Active Directory.

- The PDM has provided the SSE team with the following information:
  - o LADRA location
  - o UTAM
  - o Site specific POCs

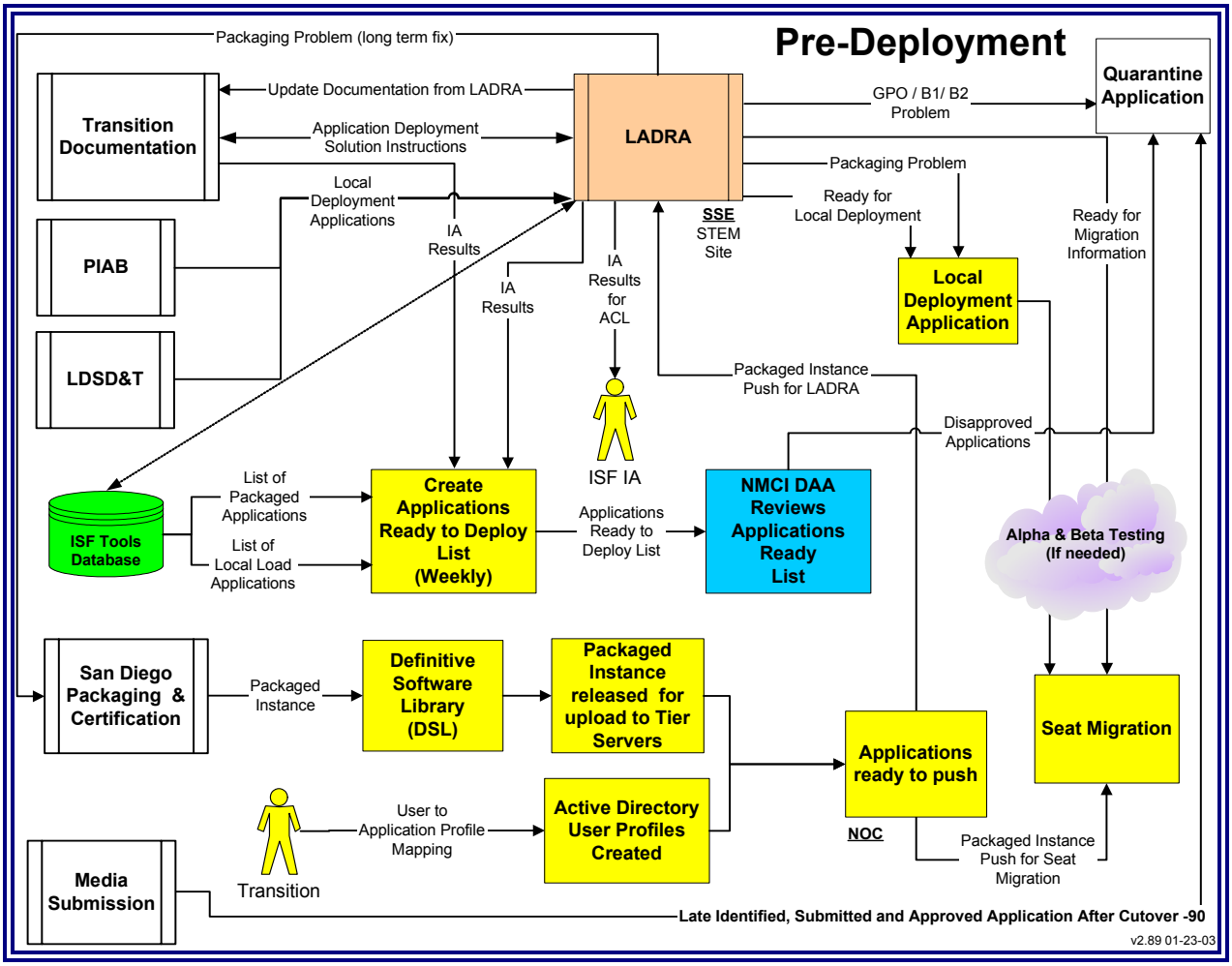


Figure 4-12. Pre-Deployment

The Pre-Deployment test is LADRA. The LADRA sub-process is detailed in Section 4.8 of this guide.

Upon successful completion of LADRA, the Legacy Applications are ready for the initial seat migration (Cutover).

NOTE: During the Pre-Deployment process, the testing and certification status is recorded and tracked in the ISF Tools Database by the SSE team.

4.8.1 Legacy Applications Deployment Readiness Activity (LADRA)

LADRA is the final pre-Cutover testing planned for all Legacy applications. LADRA is not a substitute for Alpha/Beta testing but rather a means of testing Legacy Applications' final configurations, NOC connectivity, boundary policies and migration processes and documentation prior to Cutover. Figure 4-13 depicts LADRA.

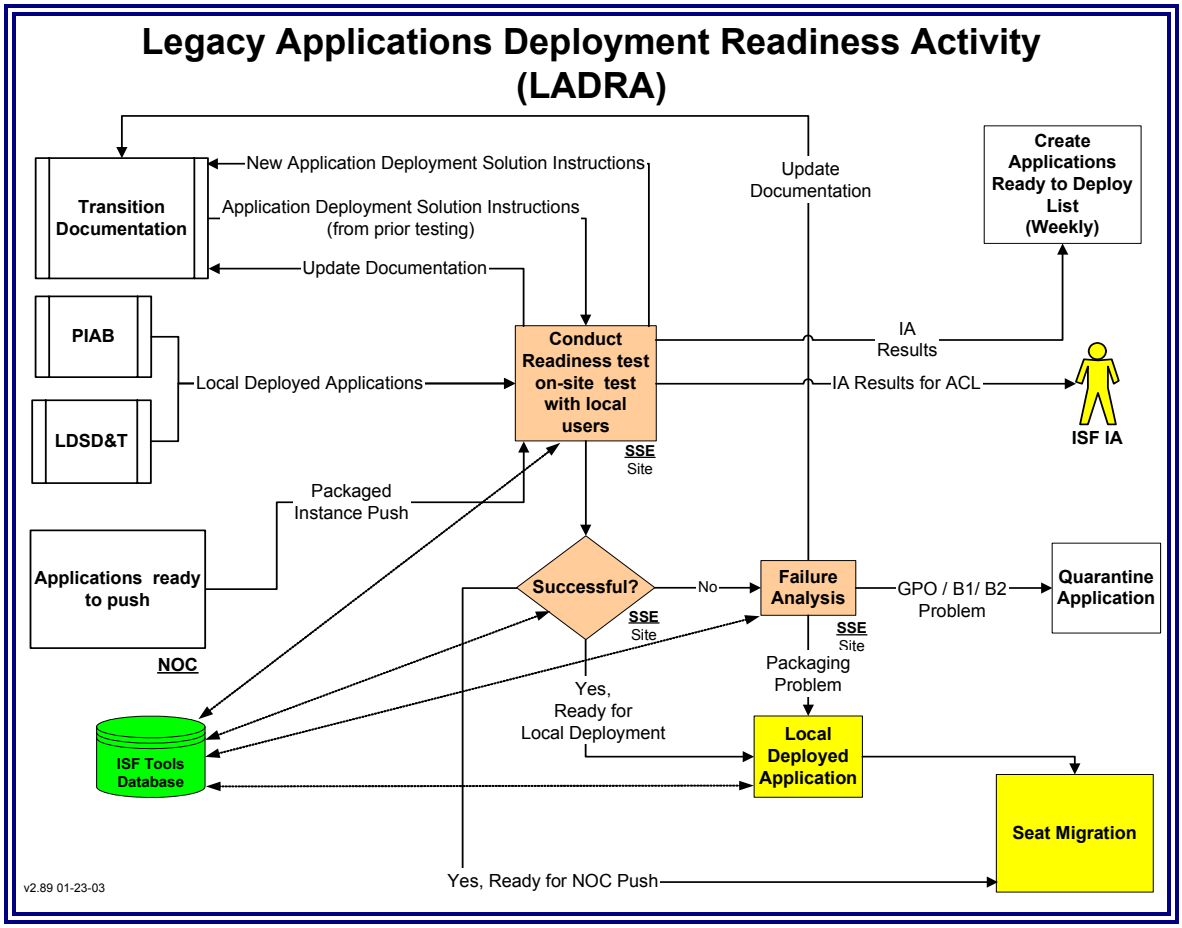


Figure 4-13. Legacy Applications Deployment Readiness Activity (LADRA)

LADRA testing is conducted by the ISF in the live NMCI environment. The goal of LADRA is to test 100% of the applications to be deployed to NMCI. In some instances, testing all applications may not be practical. The LADRA test is designed to verify the transition solutions for the Legacy Applications. The objectives of LADRA are to:

- Evaluate the performance and IA policies of Certified DSL Legacy Applications. This can include unclassified/classified COTS and GOTS in a true NMCI production environment.
- Provide on-the-job-training for select NMCI Desktop Deployment and ISF Base Ops personnel on the manual configuration of Legacy Applications.
- Ensure proper network configuration and operation.
- Evaluate migration tools.
- Evaluate Radia applications management.
- Validate migration implementation plan.
- Test print functions.

Test seats are set up for LADRA, and the NOC pushes the Legacy Applications to these seats. The ISF SSE and Transition Teams verify that the "push" occurred properly and that the applications installed. Any manual configuration changes needed for the proper installation of an application are noted and analyzed. If these configuration changes can be integrated into the Radia Instance, the application may be rejected and sent back for repackaging and NMCI Certification. If the application must be sent back for repackaging and Certification, it will be deployed locally to prevent any delay to the rollout. The packaging problem will be fixed at a later time.

The application owner/user may be asked to come to the test area to accomplish some usability tests in order to verify that an application is working properly and that it can access the server, datashare, or required Web site.

Applications can fail LADRA for the following:

- Packaging problem – kept on-site and become a locally deployed application.
- Connectivity error (B1 or B2) – Quarantined.
- GPO error – Quarantined.
- No user/tester support for application testing – Quarantined.
- Unresolved live network / application interface problems – Quarantined.

Any application failures are documented and the information is recorded in appropriate Transition Documentation.

All applications that successfully complete LADRA testing are ready for Local Deployment or NOC Push to Seat Migration (Cutover).

NOTE: During the LADRA process, the testing and certification status is recorded and tracked in the ISF Tools Database by the SSE team.

4.8.2 Quarantine

Some Legacy Applications will fail to successfully deploy into the NMCI environment during the Rapid Certification Phase of the Legacy Application Transition Process. Those applications that fail to successfully transition are referred to as Quarantined Applications. Quarantined applications will not be allowed to operate in the NMCI environment unless a solution is engineered. Quarantined applications may continue to operate in the legacy environment while they are evaluated for NMCI-compatible solutions.

Reasons for quarantine include:

- Administrative Failures:
  - NMCI Ruleset Kills that were falsely Quarantined
  - Late Submission
  - Incomplete Package Submission (Missing RFS, User, Password or Media)
  - Lack of User Support During Testing
- Technical Failures:
  - Windows 2000 Incompatibility
  - Gold Disk Interoperability
  - Deployment Failure (Network Connectivity, unsuccessful load, etc.)
  - Enterprise Group Policy Object Constraints
  - Violation of Enterprise Boundary (B1/B2) Policy

4.8.2.1 Quarantine Implementation Strategy

The following guidelines are provided (not mandated) to help determine deployment solutions for Quarantined applications based on user usage:

- Less than 1 hour per user per day = 7 users per machine
- Greater than 1 hour, but less than 3 hours per user per day = Negotiation between CTR/ISF/SIL
- Greater than 3 hours per user per day = Dual workstation
- Further considerations: Physical space for workstations, location of users, heating, ventilation, air conditioning (HVAC), power requirements, etc.

Because requirements vary between sites, deployment solutions will be done site-by-site. Actual requirements and solutions are determined through negotiations between the Site CTR, ISF Site Manager and PMO SIL.

NOTE: During the Quarantine Remediation process, the testing and certification status is recorded and tracked in the ISF Tools Database by the IATT team.

4.8.2.2 Quarantine Remediation

The standard rule followed by ISF for working on Quarantined applications is to start 30 days after Cutover Complete. Cutover Complete occurs when the last scheduled seat is rolled. ISF is not required to process Quarantined applications prior to this time if it will delay the Cutover of the site. However, if ISF has the resources available and Cutover will not be delayed, working on Quarantined applications can occur at any time. This situation is at the discretion of the ISF and is to be negotiated between the site and ISF.

Legacy Application Quarantine Remediation focuses on the resolution process of Quarantined applications in the pre and post Rapid Certification Phase. The Quarantine Remediation Process is intended for use by the IATT, STEM, Echelon II Command, Command/Site, ISF, and CDA and provides procedural guidance and a standard approach to determine the communications, interfaces, behavior, and risk level of legacy applications for development of transition strategies.

The IATT, STEM, Echelon II Command, Command/Site, ISF and CDAs will conduct a thorough assessment of the Quarantined applications and identify the required actions for NMCI transition as deemed appropriate following the NMCI DAA, Navy IO, and specific Site prioritization strategies. The IATT will provide guidance and test results to the Command/Site/CDA for the development of documentation required for transition of the application into the NMCI network.

The Quarantine Remediation principles apply to all applications and systems that have been Quarantined as a result of the NMCI Legacy Applications Rapid Certification processes. The Prioritization process identifies those high priority applications that will be resolved by the IATT and STEM. All remaining Quarantined application resolutions are the responsibility of the appropriate Echelon II Command. The following process serves as a tool to assist IATT, STEM, Echelon II Command, Command/Site, ISF, and the CDA with the evaluation of applications and systems that support the organization's vision, mission, and goals, while transitioning to NMCI.

An overview of the Quarantined Desktop Application Remediation process is provided in Figure 4-14.

The Desktop Application Quarantine Reduction Process (QRP) begins with the Prioritization process, via the various reports and lists that identify the applications that have failed to deploy to the NMCI environment. The QRP concludes with successful deployment or discontinued use of all Quarantined applications. The IATT Enterprise Quarantine Reduction Coordinator (EQRC) will oversee the execution of this effort with the IATT Quarantine Remediation Group (QRG) working with the STEM, Echelon II Commands, CDA and Sites in the execution of these processes.

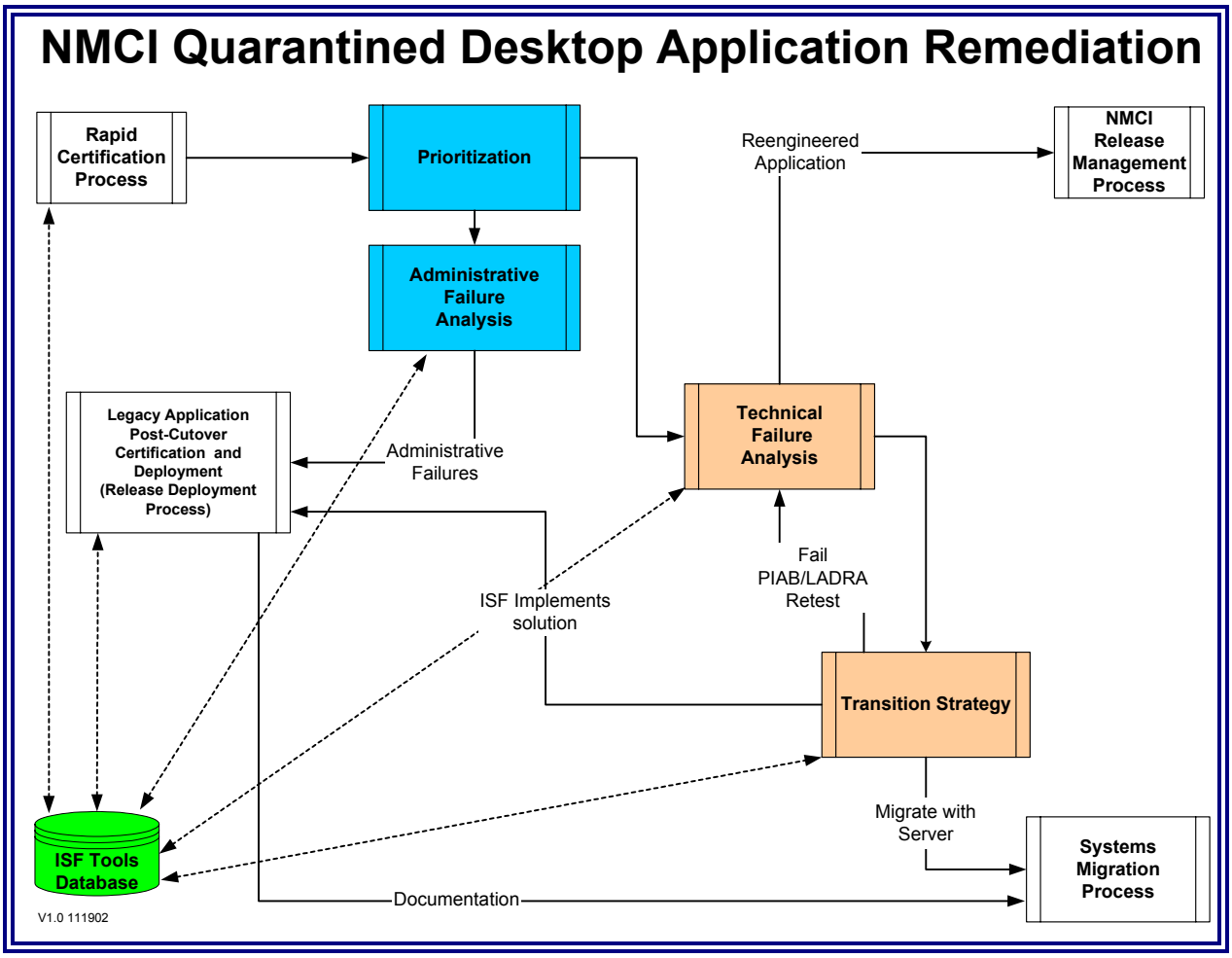


Figure 4-14. NMCI Quarantined Desktop Application Remediation

4.8.2.3 Prioritization

The QRP starts with the collection of all lists and reports dealing with Quarantine Applications. These lists and reports include:

- Admiral's Hit List – Produced by the Commander Navy Network Warfare Command (CNNWC) bi-weekly, this list highlights the Admiral's priorities for remediation.
- PMO Taskings – Produced by the NMCI Program Management Office (PMO) as needed, this list highlights the applications prioritized by the PMO.
- Customer Program Manager (CPM) Support Priority Application List (PAL) – Produced by the CPM Support Group weekly, this list identifies the top 10 priorities for a Claimant.

- NMCI DAA Report – This report is produced by the ISF identifying the test results of legacy applications.

- The IATT-DMG consolidates the above listed reports and lists on a weekly basis. All the above data is compiled into one report called the IATT Quarantine Remediation Priority List (IQRPL) for analysis.

4.8.2.4 Administrative Failure Analysis (Reasons for quarantine include):

The Administrative Failure Analysis deals with those applications that have failed to deploy in the NMCI environment for reasons other than technical. This process is primarily the responsibility of the STEM teams. Administrative failures include:

- NMCI Ruleset Kill
- Late Submittal
- Incomplete Package Submission (Missing RFS, User, Password or Media)
- Lack of user support during Usability Testing

4.8.2.5 Technical Failures

Technical Failure Determination deals with applications that have been Quarantined for one or more of the following technical failures:

- Windows 2000 (Win2K) Failure
- Gold Disk Interoperability Failure
- Deployment Failure (Network Connectivity, unsuccessful load, etc.)
- Hardware Interoperability
- Enterprise Group Policy Object (GPO) Violation
- Enterprise Boundary (B1/B2) Violation

4.8.2.5.1 Deployment Failure Transition Strategy

The ISF will attempt to resolve applications that were certified, but would not deploy due to a failure to install, operate, or function in the NMCI environment during Pre-Deployment testing. Once the ISF determines the deployment failure reason, they will implement the solution to deploy the application. ISF will retest the application via the PIAB, PIAN or NMCI Test Seat. Applications that pass testing will be deployed during the Legacy Application Post-Cutover Certification and Deployment Process (Release Deployment Process). Applications that fail testing will re-enter the Technical Failure Analysis process for further resolution.

NOTE: A more detailed explanation of the Quarantine Remediation Process is found in the Legacy Application Quarantine Remediation Guide (LAQRG).

5.0 CONCLUSION

The transition of Legacy Applications is essential to the successful implementation of NMCI. This is a monumental task requiring maximum coordination between the DON and the ISF. Every member of the DON, PMO, PEO-IT, and ISF must be committed to the success of this endeavor. It is also critical for NMCI customers to begin identification and collection of Legacy Applications and their data as early as possible in the process. Customers should also begin the process of rationalization and prioritization as soon as practicable.

The goal of the Legacy Applications process is to ensure that customers will have continued access to their critical applications after the transition to NMCI. The efforts outlined in this document will be resource-intensive, so it is imperative that NMCI customers allocate the appropriate personnel to accomplish this goal. NMCI is the accepted solution of the DON and promises a uniformly higher level of security, improved standardization, and reduced duplication, redundancy, and software support costs.

5.1 List of Resources

The definitive ISF source for customers interested in the transition of legacy application is http://www.nmci-isf.com/transition.htm.
POCs:

- SPAWAR Program Management Office – 858-537-0399
- SPAWAR Program Management Office – 619-524-7435
- Marine Corps Program Management Office – 703-784-3788 (DSN 278)
- Information Strike Force (ISF) – 619-817-3487
- Applications Enterprise Action Group (AEAG) – 703-607-5653, 703-607-5654

NEADG (for developers and CDAs) – 858-826-5168

Appendix A — Legacy Applications POA&M Template

	SITE	STEM	IATT	ISF	NMCI DAA	NADTF	PMO	ECHELON II CIO
SITE PREPARATION								
APPOINT LEGACY APPLICATIONS POC/MANAGER	CO							
OBTAIN LEGACY APPLICATIONS TRANSITION GUIDE (LATG) FROM ISF WEBSITE & REVIEW	CO, CIO, LAPOC, CTR							
ESTABLISH CONTACT WITH PMO/ISF	LAPOC							
Obtain Process Brief from PMO								
Meet ISF SM at AOR								
Meet PMO STEM at Post-AOR								
Establish contact with ISF PDM								
ESTABLISH ISF TOOLS DATABASE ACCESS								
Contact Echelon II Commander for Access	LAPOC							
OBTAIN ISF TOOLS DATABASE TRAINING								
Download ISF Database Users Guide (fm website)								
If required obtain training from Echelon II Commander or ISF Site Manager (SM) or STEM								
ONSITE TEST FACILITY PLANNING								
DETERMINE PIAB OR LADRA SEAT FACILITY REQUIREMENT								
ACQUIRE LOCAL IATO FOR TESTING CONNECTIVITY	Site DAA							
REVIEW, ACCEPT & ASSIGN PIAB OR LADRA FACILITY PLAN								
IDENTIFICATION								
CREATE IDENTIFICATION & RATIONALIZATION GAME PLAN	LAPOC							
SOCIALIZE SITE'S GAMEPLAN AND STRATEGY	LAPOC							
SURVEY USERS FOR GOTS/COTS REQUIREMENTS								
COMPARE SURVEY RESULTS AGAINST APP CATALOG IN ISF TOOL		Assist						

	SITE	STEM	IATT	ISF	NMCI DAA	NADTF	PMO	ECHELON II CIO
SELECT THOSE APPS FOUND IN APP CATALOG		Assist						
ENTER APPS NOT FOUND IN APP CATALOG IN CMD/SITE RECORD		Assist						
CREATE USER-LIST; BEGIN USER-TO- APPLICATION MAPPING		Assist						
Enter data in NOIS		Assist						
IDENTIFY/DEFINE/CREATE SITE LOAD SETS		Assist						
GATHER IN-USE PERIPHERALS, DRIVERS, SUPPLEMENTARY APPS		Assist						
COMPLETE RAW PERIPEHRAL & DRIVER LIST		Assist						
COMPLETE RATIONALIZED PERIPHERAL & DRIVER LIST		Assist						
SUBMIT RATIONALIZED PERIPHERAL & DRIVER LIST TO ISF SM		Assist						
IDENTIFY LEGACY APPLICATIONS SERVERS		Assist						
Submit data to ISF SM		Assist						
IDENTIFY DATASHARE/REACHBACK REQUIREMENTS		Assist						
Submit data to ISF SM		Assist						
RATIONALIZATION		Assist						
EXTRACT RAW APPLICATION LIST								
CATEGORIZE APPS BY TYPE AND FUNCTIONALITY		Assist						
REMOVE SIMPLE/DEVELOPER APPS FROM LIST		Assist						
APPLY NMCI APPICATION RULESET (TO NON-DEVELOPER APPS)		Assist						
PERFORM COTS & GOTS RATIONALIZATION		Assist						
APPLY AVAILABLE STANDARDS		Assist						
Apply USER TO APPLICATION MAPPING		Assist						
Complete Initial Rationalized List by Cutover -180		Assist						
COLLECTION		Assist						
COLLECT MEDIA (No Media for CBA Applications)		Assist						
COLLECT INSTALLATION INSTRUCTIONS AND TEST SCRIPTS		Assist						
GENERATE RFS FROM ISF TOOLS DATABASE		Assist						

	SITE	STEM	IATT	ISF	NMCI DAA	NADTF	PMO	ECHELON II CIO
OBTAIN TEST PLAN		Assist						
IDENTIFY/COLLECT LICENSE COPY		Assist						
No License – Obtain License or Order from CLIN23		Assist						
IDENTIFY/COLLECT DESKTOP & SERVER CONNECTIVITY (Network Diagram)		Assist						
PERFORM FINAL USER/APP/MACHINE/SERVER/PERIPHERAL MAPPING		Assist						
Submit to ISF SM		Assist						
FINALIZED RATIONALIZED LIST DUE AT Cutover -120 using ISF Tools Database		Assist						
ECHELON II COMMAND REVIEWS AND APPROVES FINAL ACCEPTED RATIONALIZED LIST								
NADTF SCRUBS FINAL ACCEPTED RATIONALIZED LIST								
KILLED Applications Removed from RationalIZED List								
FINALIZE LOAD SETS		Assist						
Submit data to ISF SM		Assist						
PREPARE ERQ	RISK MITIGATION	Assist	RISK MITIGATION					
GATHER AVAILABLE SSAA, IATO and DITSCAP DOCUMENTATION FOR IA VULNERABILITY ASSESSMENT	RISK MITIGATION	Assist	RISK MITIGATION					
MEDIA SUBMISSION		Assist						
FOR NEW APPLICATIONS TO BE CERTIFIED SUBMIT THE FOLLOWING:		Assist						
RFS		Assist		Receipt				
Network Diagram		Assist		Receipt				
Media Submitted Onsite ISF SM		Assist		Receipt				
Install Instructions and Test Plan to Onsite ISF SM		Assist		Receipt				
FOR CBA APPLICATIONS SUBMIT THE FOLLOWING:		Assist						
RFS		Assist		Receipt				
Network Diagram		Assist		Receipt				

	SITE	STEM	IATT	ISF	NMCI DAA	NADTF	PMO	ECHELON II CIO
Test Plan		Assist		Receipt				
SUBMIT ALL MEDIA TO ISF SM by Cutover -90		Assist						
REVIEW SITE'S SUBMISSION PACKAGE FOR COMPLETENESS				SM/SSE				
TESTING (All)								
San Diego Packaging and Certification				AIT				
Audit, Packaging, Usability Test, Gold Disk Testing, Quality Assurance				AIT				
Status Entry in ISF Tools Database				AIT				
Pop-In-A-NOC (PIAN)								
Audit, Packaging				AIT				
Usability Test, Gold Disk Testing, Information Assurance Testing								
Status Entry in ISF Tools Database				AIT				
Pop-In-A-Box (PIAB)		Assist		SSE				
Audit, Packaging				SSE				
Schedule and Participate in Usability Test	User/Owner	Assist		SSE				
Participate in IA Testing (B1 & B2)	User/Owner	Assist		SSE				
Gold Disk Testing	User/Owner	Assist		SSE				
Status Entry in ISF Tools Database				SSE				
Compile & Input Application Deployment Solution Instructions				SSE				
Local Deployment Solutions Development and Testing (LDSD&T)		Assist		SSE				
Audit				SSE				
Schedule and Participate in Usability Test	User/Owner	Assist		SSE				
Participate in IA Testing (B1 & B2)	User/Owner	Assist		SSE				
Gold Disk Testing	User/Owner	Assist		SSE				
Status Entry in ISF Tools Database				SSE				
Compile & Input Application Deployment Solution Instructions				SSE				
Pre-Deployment								

	SITE	STEM	IATT	ISF	NMCI DAA	NADTF	PMO	ECHELON II CIO
Legacy Applications Deployment Readiness Activity (LADRA)								
Conduct Readiness Test with Local Users	User/Owner							
Failure Analysis	User/Owner							
Create Applications Ready to Deploy List (Weekly)				SSE				
Review Applications Ready to Deploy List (Weekly)								
Package Instance loaded to DSL								
Package Instance uploaded to Tier Servers								
Create Active Directory User Profiles								
Applications Ready to Push/Local Deploy								
Seat Migration (Rollout)								

Appendix B — NMCI Standard Seat Service Contents & Navy Enterprise Standards

The following table is the contents of the NMCI Standard Seat Services (Gold Disk) at the time this guide was published. To obtain the latest Gold Disk Contents, see http://www.nmci-isf.com or http://www.nmci-isf.com/Gold_disk_contents_11.doc

Gold Disk Contents		
SERVICE	**SOFTWARE DESCRIPTION (MINIMUM VERSION)**	**VENDOR**
Basic		
Operating System	MS Windows 2000 Build 2195 SP2/SRP1	Microsoft
Office Suite	Standard Office Automation Software Included on the Gold Disk • MS Word • MS Excel • MS PowerPoint • MS Access	Microsoft
Email Client	MS Outlook 2000	Microsoft
Internet Browser	Internet Explorer MS 5.5 SP-2 128bit	Microsoft
Virus Protection	Norton A/V Corp Edition v7.5	Symantec
PDF Viewer	Acrobat Reader v.5.05	Adobe
Terminal Emulator - Host (TN3270, VT100, X-Terminal)	Reflection 8.0.5 – Web Launch Utility	WRQ
Compression Tool	Winzip v.8.1	Winzip
Collaboration Tool	Net Meeting v3.01 (4.4.3385)	Microsoft
MultiMedia	RealPlayer 8 (6.0.9.450)	RealNetworks
MultiMedia	Windows Media Player v7.01.00.3055	Microsoft
Internet Browser	Communicator 4.76	Netscape
Electronic Records Mgmt	Trim Context	Tower
Plug-ins		
Web Controls	MacroMedia Shockwave v 8.0	MacroMedia
Web Controls	Flash Player 5.0	MacroMedia
Web Controls	Apple Quicktime Movie and Audio Viewer v 5.0	Apple
Web Controls	IPIX v6,2,0,5	Internet Pictures
Security Apps		
Security	Intruder Alert v3.5	Axent
Security	ESM v5.1	Axent
Agents		
Software Management	Radia Client Connect v.2.1	Novadigm
Inventory, Remote control	Tivoli TMA v 3.71	IBM/Tivoli
Remote Connectivity (Notebooks)		
Dial-up connectivity	PAL v4.1.1.306	MCI/Worldcom
VPN	VPN Client v.3.0	Alcatel

Appendix C — Late Application Identification and Submission Process

The Late Application Identification and Submission process is a Navy responsibility.

This Late Application Identification and Submission process is extracted from the CNO messages of 03 Aug 2001 (031345Z AUG 01), 31 Aug 2001 (312137Z AUG 01) , 25 Feb 2002 (252250Z FEB 02), and 30 Sep 2002 (301245Z SEP 02).

The 30 Sep 2002 message (301245Z SEP 02) from the Navy Information Office directs all Echelon II Commands to ensure their Final Rationalized Lists of all NMCI applications (at headquarters and all subordinate Commands) are reflected in the ISF Tools Database within sixty days of the date time group of this message (29 November, 2002). Subsequent additions to the Rationalized list require the approval of the applicable FAM and Navy IO (NADTF).

This sub-process is a part of the Identification and Rationalization, Collection and Media Submission processes.

There are four combinations of legacy application identification and submission:

- An application is identified and added to the ISF Tools Database before 29 November, 2002 and submitted before the Command/Site specific media submission deadline Cutover -90.
- An application is identified after the 29 November 2002 deadline, but it is submitted before the Command/Site specific media submission deadline Cutover -90.
- An application is identified, added to the ISF Tools Database and Rationalized List before the 29 November 2002 deadline, but it is submitted after the Command/Site specific media submission deadline Cutover -90.
- An application is identified after the 29 November 2002 deadline, and it is submitted after the Command/Site specific media submission deadline Cutover -90 but prior to the start of Cutover.

Note: A legacy application's late status will jeopardize its ability to be included in the initial seat migration with those legacy applications that were not identified late.

Command/Sites' Identification Deadlines: (Per CNO message of 30 Sep 2002)

All Echelon II Commands will ensure their Final Rationalized Lists of all NMCI applications (at headquarters and all subordinate Commands) are reflected in the ISF Tools Database by 29 November 2002.

Subsequent additions to the Rationalized list require the approval of the applicable FAM and Navy IO (NADTF).

Site's Actions and Consequences

Here is what happens for each identification and submission combination:

- Identified and Submitted On-Time - An application is identified and added to the ISF Tools Database before the 29 November 2002 deadline and submitted before the Command/Site specific media submission deadline Cutover -90:
    - This is what should happen as part of the normal legacy applications transition process. The application continues through the process with no modifications or consequences.

- Identified Late and Submitted On-Time - An application is identified after the 29 November, 2002 deadline, but it is submitted before the media submission deadline Cutover -90:

    - For this Late Identified Application, the Command/Site can enter the application into the Command/Site record in the ISF Tools Database. The application will automatically be marked as late when it is added after the 29 November 2002 deadline. The application will not be added to the Applications Catalog or the Rationalized List until an approved waiver is received from the FAM and NADTF.

    - An application identified late has to be approved by the Echelon II Command. If the Echelon II Command wants the application added to the rationalized list, it must be identified to the Navy CIO (NADTF) via official Navy message. If the application is not approved by the Echelon II Command, the application is rejected and removed (unrationalized) from the FRL by the Echelon II Command.

    - If the Navy CIO (NADTF) and the FAM approve the application, the NADTF will post a status report on waivers on the NADTF website (http://cno-n6.hq.navy.mil/navcio/leg_apps.htm., indicating that the application is approved as "late." NADTF and the FAM will mark the application as "Accepted" in the ISF Tools Database. The application will move above the "line" in the Rationalized List. The application will be Quarantined and continue through the process, to be certified and processed into NMCI at a later date. If the NADTF or the FAM does not approve the application, they will mark the application "Disapproved" in the ISF Tools Database and the application will not transition into NMCI.

  Note: A rejected or Killed application will not be utilized in NMCI and **will not** be Quarantined.

- Identified On-Time and Submitted Late - An application is identified and added to the ISF Tools Database and the Rationalized List before the 29 November 2002 deadline, but it is submitted after the Command/Site specific media submission deadline Cutover -90:
    - For this Late Submitted Application, the ISF upon receiving it will indicate the application was received late in the ISF Tools Database after Cutover -90 by marking the Late Column with a "Y" for yes and showing the entry as red.

- An application identified on time but submitted late must be approved by the responsible Echelon II Command for the site transitioning to NMCI. If the Echelon II approves the application for late submission, it must be forwarded by official Navy message to the Navy CIO (NADTF) for final adjudication. If the application is not approved by the Echelon II Command, the application is rejected and removed (unrationalized) from the FRL by the Echelon II Command.

- If the Navy CIO (NADTF) approves the application, the NADTF will post a status report on waivers on the NADTF website (http://cno-n6.hq.navy.mil/navcio/leg_apps.htm). NADTF will mark the application as "Accepted" in the ISF Tools Database. The application will be Quarantined and continue through the process, to be certified and processed into NMCI at a later date. If the Navy CIO does not approve the application, NADTF will mark the application "Disapproved" in the ISF Tools Database and the application will not transition into NMCI.

Note: A rejected or Killed application will not be utilized in NMCI and **will not** be Quarantined.

- Identified Late and Submitted Late - An application is identified after the 29 November 2002 deadline, and it is submitted after the media submission deadline Cutover -90 but prior to the start of Cutover:

  - For this Late Identified Application, the Command/Site can enter the application into the Command/Site record in the ISF Tools Database. The application will automatically be marked as late when it is added after the 29 November 2002 deadline. The application will not be added to the Applications Catalog or the Rationalized List until an approved waiver is received from the FAM and NADTF.

  - An application identified late and submitted late must be approved by the Echelon II Command. If Echelon II approval is given for the late identification/submission, it must be forwarded by official Navy message to the Navy CIO (NADTF) for final adjudication. If the application is not approved by the Echelon II Command, the application is rejected and removed (unrationalized) from the FRL by the Echelon II Command.

  - If the Navy CIO (NADTF) and the FAM approve the application, the NADTF will post a status report on waivers on the NADTF website (http://cno-n6.hq.navy.mil/navcio/leg_apps.htm. indicating that the application is approved as "late." NADTF and the FAM will mark the application as "Accepted" in the ISF Tools Database. The application will move above the "line" in the Rationalized List. The application will be Quarantined and continue through the process, to be certified and processed into NMCI at a later date. If the NADTF or the FAM does not approve the application, they will mark the application "Disapproved" in the ISF Tools Database and the application will not transition into NMCI.

Note: A rejected or Killed application will not be utilized in NMCI and **will not** be Quarantined.

Applications identified and/or submitted after the start of Cutover are determined to be "emergent." Emergent applications are not considered to be legacy applications based on the NMCI contract terms. The Site and/or the Echelon II Command will be responsible for the financial implications associated with their NMCI Certification and seat migration for emergent applications.

Changes to Legacy Applications Prior to Cutover

- Changes (Updates, Patches, Mods, Upgrades, Revisions, Fixes, etc.) to Legacy Applications will be accepted and implemented prior to Cutover -45. Changes submitted after Cutover -45 would cause the entire application to be Quarantined until the change can be successfully processed. This applies only to those original applications that were in the ISF Tools Database and on the Final Rationalized List. Processing of these changes can occur once the ISF has sufficient resources available during or after Cutover. Processing these changes will not affect or delay normal rollout.

CDA Identification Deadlines

- All existing Central Design Authorities (CDAs) must have their applications identified and RFS submitted no later than 29 November 2002.
- For those CDA applications identified after the 29 November 2002 deadline, the CDA must request a waiver to the NADTF and FAM for approval and addition to the ISF Tools Database Applications Catalog.

Quarantined Applications due to Late Identification and Submission

- The standard rule followed by ISF for working on Quarantined applications is to start processing them 30 days after Cutover Complete. Cutover Complete occurs when the last scheduled seat is rolled. The ISF is not required to process Quarantined applications prior to this time if it will delay the Cutover of the site. However, if ISF has the resources available and Cutover will not be delayed, working on Quarantined applications can occur at any time. This situation is at the discretion of the ISF and is to be negotiated between the Command/Site and ISF.
- **NADTF Late Applications Approval Process**

▪ **Late Identification and Submission Waiver**

Applications that are identified and submitted late will require waiver approval from NADTF. Waiver Request is available from the NADTF website http://cno-n6.hq.navy.mil/navcio/leg_apps.htm.

Appendix D — Pertinent Naval Messages

D.1 Navy CNO Message 252250 Z FEB 02

```
Prec:        ROUTINE

 DTG:         252250Z FEB 02

 From:        CNO WASHINGTON DC//N09T/N1/N2/N3/N4/N6/N7/N8/N093/N095/

 To:          CINCPACFLT PEARL HARBOR HI//01/N6//
              CINCLANTFLT NORFOLK VA//01/N6//
              CINCUSNAVEUR LONDON UK//01/N6//
              COMUSNAVCENT//00/N6/N65/N65B//
              NAVWARCOL NEWPORT RI//00//
              COMNAVSEASYSCOM WASHINGTON DC//00/08B//00I/01/02/03/04/
              05/09/53//
              USNA ANNAPOLIS MD//00//
              BUMED WASHINGTON DC//00/CIO//
              CNET PENSACOLA FL//00/N6//
              BUPERS MILLINGTON TN//00/01EE/014//
              COMSC WASHINGTON DC//00/N6//
              COMNAVAIRSYSCOM PATUXENT RIVER MD//00/CIO/PMA-209/
              PMA-231/PMA-233/
              PMA-234/PMA-257/PMA-260/PMA-264/PMA-271//
              COMNAVSAFECEN NORFOLK VA//00//
              COMNAVRESFOR NEW ORLEANS LA//00/N6/N62//
              COMNAVLEGSVCCOM WASHINGTON DC//00//
              COMNAVSECGRU FT GEORGE G MEADE MD//00/N6//
              COMNAVSUPSYSCOM MECHANICSBURG PA//00/N6//
              COMNAVSUPSYSCOM DET NORFOLK VA//00//
              NAVSTKAIRWARCEN FALLON NV//00//
              CNR ARLINGTON VA//00//
              COMSPAWARSYSCOM SAN DIEGO CA//00/PD16/PMW164/CIO//
              NAVPGSCOL MONTEREY CA//00//
              COMNAVFACENGCOM WASHINGTON DC//00/63//
              COMOPTEVFOR NORFOLK VA//00//
              ONI WASHINGTON DC//00/N6//
              COMNAVSPECWARCOM CORONADO CA//00/N6//
              CHINFO WASHINGTON DC//00//
              DIRSSP WASHINGTON DC//00/N6//
              COMNAVMETOCCOM STENNIS SPACE CENTER MS//00/N6//
              COMNAVSPACECOM DAHLGREN VA//00/N6//
              NAVOBSY WASHINGTON DC//00//
              COMNAVDIST WASHINGTON DC//00//
              FLDSUPPACT WASHINGTON DC//00//
              NCTSI SAN DIEGO CA//00//
              PEOWTPO CHERRY PT NC//00//
              PEO CARRIERS WASHINGTON DC//00//
              PEO SURFACE STRIKE WASHINGTON DC//00//
              PEO EXW WASHINGTON DC//00//
              PEO MUW WASHINGTON DC//00//
              PEO SUB WASHINGTON DC//00//
              PEO THEATER SURFACE COMBATANTS WASHINGTON DC DET B//
              00//
              PEO THEATER SURFACE COMBATANTS WASHINGTON DC DET C//
```

PEO THEATER SURFACE COMBATANTS WASHINGTON DC DET D//
PEOASWASM PATUXENT RIVER MD//00//
PEOTACAIR PATUXENT RIVER MD//00//
COMNAVNETOPSCOM WASHINGTON DC//00/N6/N3//

Info: SECNAV WASHINGTON DC//AAUSN//
UNSECNAV WASHINGTON DC//JJJ//
USCINCPAC HONOLULU HI//J6//
USCINCJFCOM NORFOLK VA//J6//
CMC WASHINGTON DC//ALS/C4/I&L/P&R/M&RA/PP&O/AVN/IPS//
COMFLTFORCOM NORFOLK VA//01/N6//
COMMARFORLANT//G6//
COMMARFORPAC//G6//
ASSTSECNAV RDA WASHINGTON DC//JJJ//
COMSECONDFLT
COMTHIRDFLT
COMSIXTHFLT
COMSEVENTHFLT
COMNAVAIRLANT NORFOLK VA//00/N6//
COMNAVAIRPAC SAN DIEGO CA//00/06//
COMNAVSURFLANT NORFOLK VA//00/06//
COMNAVSURFPAC SAN DIEGO CA//00/06//
COMSUBLANT NORFOLK VA//00/06//
COMSUBPAC PEARL HARBOR HI//00/06//
MSCLNOLANT NORFOLK VA//00//
MSCLNOPAC PEARL HARBOR HI
COMNAVAIRWARCENWPNDIV CHINA LAKE CA//00//
NAVAIRSYSCOM CHERRY PT NC//00//
NAVFACENGCOMDET NFI PORT HUENEME CA//00//
NAVSURFWARCENDIV DAHLGREN VA//00//
NAVICP MECHANICSBURG PA//00//
NAVICP PHILADELPHIA PA//00//
COMMARFORRES//G6//
COMMARCORMATCOM ALBANY GA//G6//
COMNAVCRUITCOM MILLINGTON TN//00//
COMMARCORSYSCOM QUANTICO VA//C4/ISR/SEI//
NCTF-CND WASHINGTON DC//00/31//
NRL WASHINGTON DC//00/5500/5540/5544//
PEOSTRKWPNSUAVN PATUXENT RIVER MD//00//
DON CIO WASHINGTON DC//00//
PEO IT WASHINGTON DC//00//
MITNOC QUANTICO VA//OPS//
NAVMEDINFOMGMTCEN BETHESDA MD//42//

Subj: NMCI LEGACY APPLICATIONS TRANSITION PROCESS//

UNCLAS

MSGID/GENADMIN/CNO N09T/001-02//

SUBJ/NMCI LEGACY APPLICATIONS TRANSITION PROCESS//

REF/A/GENADMIN/CNO 09T WASHINGTON DC/061414ZJUL2001/003-01//

REF/B/GENADMIN/CNO 09T WASHINGTON DC/031345ZAUG01/005-01//

NARR/REFS A AND B ARE NAVY CIO MESSAGES 003-01 AND 005-01 AND

PROVIDE GUIDANCE FOR NMCI TRANSITION OF LEGACY APPLICATIONS AND DIRECTED A ONE-TIME INVENTORY AND REPORTING OF LEGACY APPLICATIONS AT ALL ECHELON II COMMANDS.//
POC/ALAND, DAVID/CAPTAIN/OPNAV NAVY CIO/LOC: WASHINGTON DC/TEL: 703-604-6880//

AMPN/EMAIL: ALAND.DAVID@HQ.NAVY.MIL//

RMKS/1. EXECUTIVE SUMMARY. THE TRANSITION OF LEGACY APPLICATIONS TO NMCI IS A CRITICAL STEP FORWARD IN OUR ABILITY TO REALISTICALLY PERFORM INFORMATION RESOURCE MANAGEMENT. IT IS A LEADERSHIP ISSUE WHICH REQUIRES YOUR IMMEDIATE AND DIRECT ATTENTION. STATUS OF EACH ECHELON II COMMAND'S IDENTIFICATION, RATIONALIZATION, AND SUBMISSION OF APPLICATIONS FOR CERTIFICATION AND ACCREDITATION WILL BE REPORTED TO THE CNO AND SECNAV ON A WEEKLY BASIS. THIS MESSAGE BOTH MANDATES THE USE OF THE LEGACY APPLICATION TRANSITION GUIDE (LATG) AND MODIFIES LATG, PROVIDING DETAILED SUBMISSION DATES AND PROCEDURES THAT MUST BE FOLLOWED. THE MODIFICATION OF THE LATG SEPARATES THE NMCI CERTIFICATION PROCESS FROM THE FINAL ACCREDITATION PROCESS AND DELIVERS APPLICATIONS WHICH WILL OPERATE ON NMCI SEATS WITHOUT COMPROMISING SECURITY. REGRET THE LENGTH OF MESSAGE BUT THIS PROCESS CHANGE REQUIRES DETAIL AND CLARITY.

2. ECHELON II COMMANDERS ARE EACH RESPONSIBLE FOR THE IDENTIFICATION, RATIONALIZATION, AND SUBMISSION FOR CERTIFICATION AND ACCREDITATION OF THEIR APPLICATIONS. A CENTRAL DATABASE HAS BEEN ESTABLISHED FOR ALL NAVY APPLICATIONS. ACCESS TO THE DATABASE IS VIA A WEBSITE REQUIRING A USER PASSWORD. A SEPARATE MESSAGE WILL PROVIDE INFORMATION ON HOW ACCESS TO THE DATABASE CAN BE OBTAINED VIA EACH INDIVIDUAL'S ECHELON II COMMAND TO READ AND/OR WRITE TO THE DATABASE. A REVIEW OF THIS DATABASE INDICATES THAT MOST NMCI INCREMENT 1.0 AND 1.5 COMMANDS HAVE NOT COMPLETED THE REQUIRED DATA SUBMISSION IN SUPPORT OF NMCI IMPLEMENTATION. ADDITIONALLY, MOST COMMANDS SCHEDULED FOR NMCI INCREMENT 2.0 AND BEYOND HAVE SUBMITTED INCOMPLETE DATA WHICH COULD IMPACT NMCI IMPLEMENTATION. SITE TRANSITION EXECUTION MANAGER (STEM), ENTERPRISE APPLICATIONS GROUP FOR LEGACY & EMERGING (EAGLE) AND INFORMATION ASSURANCE TIGER TEAM (IATT) PERSONNEL HAVE BEEN FIELDED TO ASSIST TRANSITIONING SITES WITH THIS TASK. HOWEVER, THE SPEED AT WHICH LEGACY APPLICATIONS ARE IDENTIFIED, RATIONALIZED (REDUCED IN NUMBER), TESTED, CERTIFIED, AND ACCREDITED MUST BE IMPROVED. THERE ARE THREE KEYS TO IMPROVING THIS PROCESS. THE FIRST IS TO ENSURE EACH ECHELON II COMMAND MAINTAINS THEIR APPLICATION DATA CURRENT AND ACCURATE IN THE APPLICATION DATABASE TO ELIMINATE DUPLICATION OF EFFORT ACROSS THE NAVY ENTERPRISE. APPLICATIONS CERTIFIED AND ACCREDITED UNDER THE LATG PROCESS DO NOT REQUIRE DUPLICATE CERTIFICATION AND ACCREDITATION AT SUBSEQUENT COMMANDS/SITES. (REQUEST FOR SERVICE (RFS) SUBMISSION IS STILL REQUIRED BY SUBSEQUENT COMMANDS/SITES TO DOCUMENT APPLICATION USE AND PREVIOUSLY ACCOMPLISHED CERTIFICATION.) THE SECOND KEY IS A REDUCTION IN THE NUMBER OF LEGACY APPLICATIONS ACHIEVED BY ECHELON II RATIONALIZATION AND NAVY TRIAGE PROCESS. (DATA COLLECTED THUS FAR SHOWS APPROXIMATELY 10-20 PERCENT OF ALL APPLICATIONS CURRENTLY CERTIFIED AND ACCREDITED DO NOT HAVE ANY IDENTIFIED USERS, WHICH HAS RESULTED IN A NEEDLESS EXPENDITURE OF SCARCE RESOURCES.) THE THIRD KEY IS A REDUCTION IN THE REQUIREMENTS FOR INCLUDING LEGACY APPLICATIONS AT NMCI SEAT CUTOVER, BUT NOT A REDUCTION IN REQUIREMENTS FOR LEGACY APPLICATION ACCREDITATION. IN ORDER TO

REDUCE THE IMPACT TO NMCI SEAT ROLLOUT, THE APPLICATION TRANSITION PROCESS IS MODIFIED PER PARAGRAPH 3 AND ACTION IDENTIFIED IN PARAGRAPH 4 IS MANDATORY.

3. LEGACY APPLICATION TRANSITION PROCESS MODIFICATION. THE FOLLOWING PROCESS MODIFICATIONS ARE EFFECTIVE IMMEDIATELY AND SHALL BE FOLLOWED IN CONJUNCTION WITH THE LATG:

A. GENERAL: THE CURRENT LEGACY APPLICATION PROCESS ENTAILS SITE IMPLEMENTATION VICE COMMAND IMPLEMENTATION DURING THE LEGACY APPLICATION IDENTIFICATION AND THE RATIONALIZATION PROCESSES AND THE COMPLETION OF THE CERTIFICATION PROCESS (COMPATIBILITY WITH THE NMCI OPERATING ENVIRONMENT) AND THE SYSTEM SECURITY AUTHORIZATION AGREEMENT (SSAA) PRIOR TO COMMENCING CUTOVER OF SEATS. THE NEW PROCESS REQUIRES ECHELON II CHAIN OF COMMAND (COC) INVOLVEMENT DURING THE IDENTIFICATION AND THE RATIONALIZATION PROCESSES AND DIVIDES THE CERTIFICATION PROCESS INTO TWO PHASES, THE NMCI CERTIFICATION PHASE AND THE RISK MITIGATION (ACCREDITATION) PHASE.
B. IDENTIFICATION AND RATIONALIZATION: NEW PROCESS REQUIRES SUBORDINATE COMMANDS TO SUBMIT THEIR RATIONALIZED LIST OF APPLICATIONS VIA THEIR COC TO THEIR ECHELON II FOR RATIONALIZATION ACROSS THE ECHELON II'S ENTERPRISE. IT REQUIRES A WEEKLY REPORTING OF EACH COMMAND'S PROGRESS IN COMPLETING SUBMISSION REQUIREMENTS FOR THE CERTIFICATION PROCESS.
C. NMCI CERTIFICATION: IN THE NEW PROCESS THE NMCI CERTIFICATION PHASE INCLUDES THE DEVELOPMENT OF RATIONALIZED LISTS OF APPLICATIONS, THE SUBMISSION OF REQUESTS FOR SERVICE (RFS) AND MEDIA FOR THOSE APPLICATIONS, THE SUBMISSION OF THE CERTIFICATION PHASE ENGINEERING REVIEW QUESTIONNAIRE (ERQ), THE ACTUAL CERTIFICATION TESTING OF THE APPLICATION, AND THE SUBMISSION OF AN IATT VULNERABILITY ASSESSMENT LETTER TO THE NMCI DESIGNATED APPROVAL AUTHORITY (DAA) (CAPTAIN BOB WHITKOP, COMMANDER NAVY NETWORK OPERATIONS COMMAND (CNNOC)). THE NMCI CERTIFICATION PROCESS CULMINATES IN THE ISSUANCE OF AN INTERIM AUTHORITY TO OPERATE (IATO) LETTER FROM THE NMCI DAA. THE IATO WILL CONTAIN LIMITATIONS ON THE OPERATION OF EACH APPLICATION AND REQUIRE INFORMATION ASSURANCE RISK MITIGATION ACTIONS TO BE ACCOMPLISHED WITHIN TIME SPECIFIED IN PARAGRAPH 3.D.
D. CERTIFICATION PROCESS CHANGES: THE PACING FACTOR FOR MUCH OF THE NMCI CERTIFICATION PROCESS WILL CONTINUE TO RELY ON OBTAINING THE RFS, MEDIA, AND COMPLETION OF THE ERQ FOR EACH COMMAND'S APPLICATIONS AT EACH SITE. IT IS ESSENTIAL THAT BOTH THE APPLICABLE ECHELON II COMMANDS AND THE SITE ENSURE THIS DATA IS SUBMITTED IN A TIMELY MANNER IN ORDER TO SUPPORT THE NMCI IMPLEMENTATION SCHEDULE. THE NMCI CERTIFICATION ERQ AND THE RISK MITIGATION (ACCREDITATION) ERQ INCLUDE ALL THE DATA REQUIREMENTS OF THE ORIGINAL ERQ. HOWEVER, THE NMCI CERTIFICATION ERQ HAS BEEN SIGNIFICANTLY REDUCED IN SIZE AND COMPLEXITY TO EXPEDITE THE SEAT CUTOVER PROCESS, WHILE COLLECTING THE NECESSARY INFORMATION TO ENSURE NETWORK SECURITY IS MAINTAINED AT CUTOVER. THE NMCI CERTIFICATION TESTING HAS ALSO BEEN STREAMLINED. EACH APPLICATION WILL UNDERGO AN ON SITE POP-IN-A-BOX (PIAB) TEST TO ENSURE COMPATIBILITY WITH THE MICROSOFT WIN2K OPERATING SYSTEM, DESKTOP GROUP POLICY OBJECT (GPO), SECURITY COMPONENTS AND SETTINGS. THE PIAB TESTING WILL ALSO PROVIDE CONNECTIVITY REQUIREMENTS BETWEEN CLIENT AND SERVER AT THE PROTOCOL, SERVICE AND PORT LEVEL. ADDITIONAL PERSONNEL AND EQUIPMENT WILL BE ASSIGNED BY THE PMO AND

THE NMCI CONTRACTOR TO THE EXISTING TEAMS IN ORDER TO CONDUCT THIS ON SITE PIAB TESTING AND DOCUMENTATION AT A GREATER NUMBER OF SITES CONCURRENTLY. BASED ON THIS INFORMATION GAINED FROM THE PIAB TESTING, THE IATT WILL PROVIDE A RISK ASSESSMENT OF EACH APPLICATION AS FOLLOWS:

-- LOW RISK - COMPLIANT WITH NAVY/MARINE CORPS ENCLAVE PROTECTION POLICY AND ACCREDITED.

-- MEDIUM RISK - OUTBOUND TCP COMMUNICATION REQUIREMENTS NOT ALREADY PERMITTED.

-- HIGH RISK - TWO WAY IP/TCP/UDP COMMUNICATION REQUIREMENTS NOT ALREADY PERMITTED.

-- VERY HIGH RISK - UNACCEPTABLE PROTOCOLS OR REQUIREMENTS. MANDATORY KIOSK MITIGATION UNTIL DISCONTINUED OR REENGINEERED. THESE RISKS WILL BE CAPTURED BY THE ON-SITE IATT REPRESENTATIVES AND FORWARDED TO THE NMCI DAA IN THE VULNERABILITY ASSESSMENT LETTER. WHEN ALL CERTIFICATION TESTING RESULTS FOR A SITE ARE AVAILABLE TO THE NMCI DAA, HE WILL ISSUE A TYPE ACCREDITED BOUNDARY 2 FIREWALL POLICY FOR THE SITE AND ISSUE AN IATO COVERING THE SUITE OF APPLICATIONS AT THAT SITE. IN ADDITION TO THE VULNERABILITY ASSESSMENT RESULTS DISCUSSED ABOVE, THE IATO WILL CONSIDER THE STATE OF AVAILABLE SSAA DOCUMENTATION FOR EACH APPLICATION IN ACCORDANCE WITH THE FOLLOWING BOUNDARY 1 FIREWALL COMPLIANCE CATEGORIES:

- CATEGORY 1 - CLIENT APPLICATION IS NMCI CERTIFIED AND USES TRUSTED COMMUNICATIONS WITH THE SUPPORTING SERVER. EITHER THE SERVER APPLICATION OR BOTH CLIENT AND SERVER PORTIONS OF THE APPLICATION HAVE CERTIFICATION AND ACCREDITATION (C&A) PACKAGES AND CAN BE MOVED INTO NMCI TRUSTED ENCLAVE. SSAA PACKAGE IS COMPLETE AND THE APPLICATION IS ACCREDITED.

- CATEGORY 2 - CLIENT APPLICATION IS NMCI CERTIFIED, BUT CONCERNS EXIST ABOUT COMMUNICATIONS WITH THE SERVER BECAUSE OF A LACK OF COMPLETED DOCUMENTATION (NO DEPARTMENT OF DEFENSE (DOD) C&A.) SERVER APPLICATION IS NMCI CERTIFIED, BUT CONCERNS EXIST WITH THE SERVER'S COMMUNICATION WITH OTHER SERVERS AND/OR CLIENTS BECAUSE OF THE LACK OF COMPLETED DOCUMENTATION (NO DOD C&A.) NO BOUNDARY 2 MODIFICATIONS ARE REQUIRED. RISK IS MINIMIZED IF BOTH CLIENT AND SERVER ARE PLACED WITHIN NMCI ENCLAVE VICE LEAVING THE SERVER OUTSIDE THE NMCI ENCLAVE.

- CATEGORY 3 - CLIENT IS NMCI CERTIFIED, BUT SERVER HAS UNTRUSTED COMMUNICATION REQUIREMENTS TO NON-NMCI USERS FOR THE RISK MITIGATION (ACCREDITATION) PHASE OR LONGER. SERVER APPLICATION IS NMCI CERTIFIED, BUT THE SERVER HAS UNTRUSTED COMMUNICATION REQUIREMENTS TO NON-NMCI SERVERS AND/OR USERS FOR THE RISK MITIGATION (ACCREDITATION PHASE OR LONGER. BOUNDARY 2 FIREWALL MODIFICATION IS REQUIRED.

- CATEGORY 4 - CLIENT APPLICATION MAY OR MAY NOT BE CERTIFIED, AND THERE IS UNTRUSTED COMMUNICATIONS BETWEEN CLIENT AND SERVER OR SERVER AND SERVER OR APPLICATION CLIENT/SERVER IS ACCESSIBLE TO THE GENERAL PUBLIC. NO DOD C&A SYSTEM CAN EITHER BE SUNSET-ED OR KIOSKED. A RULE SET GOVERNING SUPPORT FOR KIOSKED APPLICATIONS WILL BE PROVIDED SEPARATELY. BASED ON BOUNDARY 1 FIREWALL COMPLIANCE CATEGORY AND THE RISK LEVEL, THE NMCI DAA WILL ISSUE AN IATO REQUIRING SPECIFIC ACTIONS AND LIMIT THE AUTHORITY TO OPERATE FOR A SPECIFIED TIME PERIOD AS FOLLOWS:

CATEGORY 1 - LENGTH OF AUTHORITY TO OPERATE (ATO) (NORMALLY 3 YEARS).

CATEGORY 2 - ONE YEAR

CATEGORY 3 - SUBMIT PLAN OF ACTION MILESTONES (POA&M) FOR

MIGRATION VIA APPLICABLE ECHELON II COMMAND WITHIN SIX MONTHS TO NAVY CIO FOR APPROVAL/DISAPPROVAL AND ANNUAL REVIEW.
CATEGORY 4 - POA&M SUBMITTED FOR MITIGATION/MIGRATION VIA APPLICABLE ECHELON II DUE WITHIN THREE MONTHS TO NAVY CIO. MIGRATION/TERMINATION MUST BE COMPLETED WITHIN NINE MONTHS.
E. RISK MITIGATION (ACCREDITATION): THE SECOND PHASE OF THE PROCESS COMMENCES AFTER NMCI SEAT CUTOVER AND INVOLVES THE COMPLETION OF THE RISK MITIGATION (ACCREDITATION) ERQ, FURTHER DEVELOPMENT OF RISK MITIGATION STRATEGIES, SUBMISSION OF POA&M FOR EACH APPLICABLE APPLICATION IAW IATO REQUIREMENTS, EXECUTION OF APPLICATION MITIGATION ACTION AND COMPLETION OF SSAA DOCUMENTATION. FAILURE TO COMPLETE REQUIRED MITIGATION ACTIONS (SUBMIT POA&M AND MEET TIMELINES) WILL RESULT IN EITHER DENIAL OF APPLICATION USE ON NMCI BY THE NAVY CIO OR POTENTIAL ADDITIONAL MITIGATION REQUIREMENTS. THE PRIMARY TASKS IN THIS PHASE ARE THE MITIGATIONS OF THE RISKS IDENTIFIED DURING THE CERTIFICATION PHASE AND THE COMPLETION OF THE SSAA DOCUMENTATION REQUIRED FOR CERTIFICATION. THERE HAVE BEEN MANY TECHNIQUES ALREADY DEVELOPED BY THE NMCI CONTRACTOR (INFORMATION STRIKE FORCE (ISF)) FOR CATEGORY 3 APPLICATIONS TO MITIGATE RISKS UNTIL THE SERVER CAN BE TRANSITIONED INTO THE NMCI ENCLAVE. COMPLETION OF RISK MITIGATION IS THE RESPONSIBILITY OF THE APPLICABLE ECHELON II COMMAND, INCLUDING APPLICABLE SUBORDINATE COMMANDS, THE CENTRAL DESIGN ACTIVITY (AS DESIGNATED IN PARAGRAPH 4.B) AND THE ISF. SSAA DOCUMENTATION IS SUBMITTED BY ECHELON II COMMAND OR CDA, AS APPROPRIATE, TO NMCI PROGRAM MANAGEMENT OFFICE (PMO) FOR INITIAL REVIEW AND EVALUATION PRIOR TO SUBMISSION TO THE NMCI DAA FOR APPROVAL. FOR CATEGORY 4 APPLICATIONS, A RECOMMENDATION TO MIGRATE OR TERMINATE THE APPLICATION WILL BE MADE AND APPROVED BY THE NAVY CIO. FOR ALL APPLICATIONS THAT ARE TO REMAIN IN THE NMCI, THE SSAA DOCUMENTATION WILL BE DEVELOPED BY THE ECHELON II COMMAND OR CDA, AS APPROPRIATE, AND SUBMITTED TO NMCI PMO FOR INITIAL REVIEW AND EVALUATION PRIOR TO SUBMISSION TO THE NMCI DAA FOR APPROVAL.
F. NAVY TRIAGE PROCESS: AN APPLICATION TRIAGE PROCESS, WHICH WILL BE DESIGNED TO REDUCE THE OVERALL NUMBER OF NAVY APPLICATIONS, WILL RUN CONCURRENTLY WITH NMCI CERTIFICATION AND THE RISK MITIGATION (ACCREDITATION) PHASES AT THE ECHELON II AND NAVY CIO LEVEL. THE PRODUCT OF THE NMCI CERTIFICATION PHASE, BOUNDARY 1 FIREWALL COMPLIANCE CATEGORY AND RISK LEVEL, WILL BE USED TO ESTABLISH PRIORITIES AND IDENTIFY APPLICATIONS FOR ELIMINATION DURING THE TRIAGE PROCESS. THIS PROCESS WILL BE ADDRESSED SEPARATELY.

4. ACTION AND RESPONSIBILITIES. IN ORDER FOR THE MODIFIED PROCESS DEFINED IN PARAGRAPH 3 TO BE EFFECTIVE THE FOLLOWING SPECIFIC ACTION AND RESPONSIBILITIES ARE REQUIRED:
A. ECHELON II ARE RESPONSIBLE TO ENSURE THEY AND THEIR SUBORDINATE COMMANDS COMPLY WITH THE FOLLOWING:
(1) 60 DAYS PRIOR TO AOR, THE APPLICABLE COMMAND DELIVERS THE COMPLETED LIST OF ALL COTS AND GOTS APPLICATIONS REQUIRED TO OPERATE ON NMCI AND RATIONALIZED BY THEIR ECHELON II COMMAND. 50 PERCENT OF ALL GOTS APPLICATIONS MUST BE DELIVERED AND ACCEPTED BY THE ISF FOR CERTIFICATION.
(2) 45 DAYS PRIOR TO AOR, THE APPLICABLE COMMAND SHALL HAVE 75 PERCENT OF IDENTIFIED APPLICATIONS (COTS AND GOTS) DELIVERED AND ACCEPTED FOR CERTIFICATION.
(3) 30 DAYS PRIOR TO AOR, THE APPLICABLE COMMAND SHALL ENSURE ALL REMAINING IDENTIFIED APPLICATIONS (COTS AND GOTS) MUST BE SUBMITTED

AND ACCEPTED FOR CERTIFICATION. APPLICATIONS NOT SUBMITTED BY THIS DEADLINE WILL NOT TRANSITION TO NMCI ON THE SCHEDULED CUTOVER DATE.
(4) 14 DAYS PRIOR TO START OF CUTOVER, ALL APPLICATIONS REQUIRED FOR CUTOVER ARE CERTIFIED.
(5) ALL INCREMENT 1.0 COMMANDS MUST HAVE COMPLETED SUBMISSION OF THEIR FINALIZED RATIONALIZED APPLICATION LIST TO NMCI PMO. THE APPROPRIATE ECHELON II COMMAND SHOULD HAVE PREVIOUSLY APPROVED THIS RATIONALIZED LIST OR DO SO NLT 21 MARCH 2002.
(6) ALL INCREMENT 1.5 COMMANDS MUST HAVE THEIR RATIONALIZED LIST OF APPLICATIONS SUBMITTED VIA THEIR APPLICABLE ECHELON II COMMAND NLT 21 MARCH 2002.
(7) APPLICATIONS SHALL BE SUBMITTED AS NOTED ABOVE USING THE REQUEST FOR SERVICE (RFS) AND CERTIFICATION PHASE ERQ. ALL DATA ELEMENTS IDENTIFIED IN THE RFS AND IN THE CERTIFICATION PHASE AND THE RISK MITIGATION (ACCREDITATION) PHASE ERQ ARE MANDATORY IN ORDER FOR THIS SUBMISSION TO BE CONSIDERED COMPLETE.
B. DESIGNATION OF CDA: CRITICAL TO THE LEGACY APPLICATION PROCESS IS THE ASSIGNMENT OF RESPONSIBILITY FOR EVERY APPLICATION TO BE CERTIFIED OR ACCREDITED. THIS MESSAGE ASSIGNS RESPONSIBILITIES TO CENTRAL DESIGN ACTIVITIES (CDA) AND DETAILS THE PROCESS TO ASSIGN CDA RESPONSIBILITIES WHEN A DESIGNATED CDA DOES NOT EXIST. IN ORDER TO EXPEDITE THE CERTIFICATION AND ACCREDITATION PROCESS, CDA(S) FOR APPLICATIONS WHICH EXIST AT MORE THAN ONE SITE, SHALL SUBMIT SSAA DOCUMENTATION FOR THE APPLICABLE APPLICATION ONCE VICE REQUIRING DUPLICATION OF CDA RESPONSIBILITIES AT MULTIPLE SITES BY MULTIPLE ECHELON II COMMANDS. CDA HAS PRINCIPAL RESPONSIBILITY FOR DESIGN, DEVELOPMENT, DOCUMENTATION, AND LIFE CYCLE MAINTENANCE OF APPLICATIONS, INCLUDING INITIAL PRODUCT DELIVERY AND DISTRIBUTION OF UPDATES. ADDITIONALLY, CDA(S) RESOURCE AND MAINTAIN HELP DESK SERVICES FOR THEIR APPLICATIONS. THE PRIMARY DON CDA(S) ARE CONTROLLED BY NAVSEA, NAVAIR, SPAWAR, NAVSUP, NAVFAC, CNET, MARINE CORPS SYSTEMS COMMAND AND DISTRIBUTED TO SOME OF THEIR SUBORDINATE COMMANDS (E.G. NAVSUP HAS FLEET MATERIALS SUPPORT OFFICE (FMSO) PROVIDE THEIR CDA RESPONSIBILITIES). THE FOLLOWING CATEGORIES OF APPLICATIONS AND THEIR ASSOCIATED CDA IDENTIFICATION AND DESIGNATION RESPONSIBILITY ARE ASSIGNED:
(1) NAVY SYSTEM COMMAND DEVELOPED GOTS - APPLICABLE SYSCOM IS RESPONSIBLE FOR IDENTIFICATION, DESIGNATION OF THE CDA AND ENSURING SUBSEQUENT CDA RESPONSIBILITIES ARE ACCOMPLISHED IAW THIS MESSAGE.
(2) MARINE CORPS SYSTEM COMMAND DEVELOPED GOTS - APPLICABLE NAVY ECHELON II IS RESPONSIBLE FOR REPORTING THE APPLICATION ASSOCIATED SYSCOM TO NAVY CIO, MARINE CORPS CIO OFFICE AND NMCI PMO. THE NAVY CIO WILL WORK WITH MARINE CORPS CIO OFFICE AND NMCI PMO FOR CDA IDENTIFICATION, DESIGNATION OF THE CDA AND THE CDA'S COMPLETION OF REQUIRED ACTION.
(3) INDIVIDUAL COMMAND DEVELOPED GOTS - APPLICABLE ECHELON II IS RESPONSIBLE FOR IDENTIFICATION, DESIGNATION OF THE CDA AND THE CDA'S COMPLETION OF REQUIRED ACTION.
(4) OTHER SERVICE/JOINT/OSD AND OTHER AGENCY DEVELOPED GOTS - APPLICABLE ECHELON II IS RESPONSIBLE FOR IDENTIFICATION OF THE APPLICATION AND ITS SOURCE TO NAVY CIO AND NMCI PMO. THE NAVY CIO WILL WORK WITH DON CIO AND NMCI PMO FOR IDENTIFICATION AND DESIGNATION OF THE CDA AND THE CDA'S COMPLETION OF REQUIRED ACTION.
(5) NON-GOVERNMENT, NON-COMMERCIAL PRODUCTS - APPLICABLE ECHELON II WHOSE SUBORDINATE COMMAND PURCHASED THE PRODUCT FOR USE IS RESPONSIBLE FOR IDENTIFICATION AND DESIGNATION OF THE CDA AND THE CDA'S COMPLETION OF REQUIRED ACTION.

(6) COMMERCIAL PRODUCTS (COTS) - APPLICABLE ECHELON II WHOSE SUBORDINATE COMMAND PURCHASED THE PRODUCT FOR USE IS RESPONSIBLE FOR IDENTIFICATION AND DESIGNATION OF THE CDA AND THE CDA'S COMPLETION OF REQUIRED ACTION. FOR APPLICATIONS CONTAINED IN THE NMCI BASIC DESKTOP SEAT, IDENTIFICATION AND DESIGNATION OF CDA IS NOT REQUIRED. IN THE FUTURE, AS ENTERPRISE APPLICATIONS ARE DESIGNATED AND CENTRALLY PURCHASED CDA RESPONSIBILITIES WILL BE ASSIGNED TO THE VENDOR AND INCLUDED IN THE ACQUISITION AGREEMENT.
C. ECHELON II AND CDA RESPONSIBILITIES: AS APPLICABLE, EACH ECHELON II COMMAND IS RESPONSIBLE FOR ENSURING THEIR CDA(S) SUBMIT THE APPLICATION SSAA DOCUMENTATION TO NMCI PMO. FOR EXAMPLE, THE CDA FOR THE NAVAL AIR LOGISTICS COMMAND MANAGEMENT INFORMATION SYSTEM (NALCOMIS) IS SPAWAR SO SPAWAR SHOULD ENSURE THE CDA FOR NALCOMIS COMPLIES WITH THE REQUIREMENTS OF THIS MESSAGE. AS A JOINT EXAMPLE, THE CDA FOR THE DEFENSE MESSAGE SYSTEM (DMS) IS DISA, SO ECHELON II REPORTS THE SOURCE OF DMS AS DISA AND THE NAVY CIO WILL WORK WITH DON CIO TO ENSURE DISA HAS THEIR DMS CDA COMPLY WITH THE REQUIREMENTS OF THIS MESSAGE. THESE KNOWN CDA(S) SHOULD BE PROVIDING THE REQUIRED SSAA DOCUMENTATION AND THE NMCI PMO WILL CONDUCT AN INITIAL REVIEW OF THE SSAA FOR CONSIDERATION AS ADEQUATE DOCUMENTATION FOR ALL NMCI COMMAND AND SITE IMPLEMENTATIONS. THIS CDA SUBMITTED SSAA DOCUMENTATION WILL BE EVALUATED AND ASSIGNED THE FOLLOWING STATUS: (A) SATISFACTORY AS A SSAA FOR NMCI, OR (B) NOT SATISFACTORY AS A SSAA FOR NMCI BUT DOES INCLUDE THE NECESSARY INFORMATION FOR COMPLETION OF THE NMCI CERTIFICATION PROCESS, OR (C) INCOMPLETE. SATISFACTORY SSAA'S WILL BE SUBMITTED TO THE NMCI CERTIFICATION AND ACCREDITATION REVIEW PANEL (NCARP) FOR ENTERPRISE ACCREDITATION. IF THIS CDA SUBMITTED SSAA DOCUMENTATION IS NOT A SATISFACTORY SSAA FOR NMCI OR IS INCOMPLETE, NMCI PMO WILL REPORT THIS TO THE NMCI DAA, THE LOCAL DAA(S) AND CAUSE A FORMAL MESSAGE TO BE PREPARED TASKING THE APPLICABLE CDA TO TAKE ACTION TO ENSURE MINIMUM REQUIREMENTS FOR SEAT CUTOVER ARE COMPLETED IMMEDIATELY. THE CDA MUST ENSURE SUBSEQUENT SSAA DOCUMENTATION IS COMPLETED IN ACCORDANCE WITH THE IATO TIME REQUIREMENTS FOR THE SPECIFIC APPLICATION. THE FOLLOWING SPECIFIC ACTION AND RESPONSIBILITIES NEED TO BE FOLLOWED BY THE CDA(S):
- MUST HAVE COMPLETED SUBMISSION OF AN RFS FOR EACH APPLICATION NLT 21 MARCH 2002 USING THE NMCI APPLICATION DATABASE. (THE 21 MARCH 2002 DATE DOES NOT APPLY TO AN APPLICATION WHICH NEVER HAD A DESIGNATED CDA. FOR THESE APPLICATIONS, THE NEWLY DESIGNATED CDA SHOULD PROVIDE THE RFS DOCUMENTATION NLT 11 MAY 2002.)
- MUST HAVE COMPLETED SUBMISSION OF ALL CLIENT MEDIA TO THE ISF NLT 21 APRIL 2002. (THE 21 APRIL 2002 DATE DOES NOT APPLY TO AN APPLICATION WHICH NEVER HAD A DESIGNATED CDA. FOR THESE APPLICATIONS, THE NEWLY DESIGNATED CDA SHOULD PROVIDE THE CLIENT MEDIA NLT 11 MAY 2002.)
- FOR SUBSEQUENT UPGRADES/PATCHES TO EXISTING APPLICATIONS, MUST SUBMIT AN RFS USING THE NMCI APPLICATION DATABASE AND SUBMIT MEDIA TO THE ISF FOR CERTIFICATION. EACH CDA IS RESPONSIBLE FOR INDEPENDENT CERTIFICATION AND ACCREDITATION OF ANY CHANGES TO THEIR APPLICATIONS AS DESIGNATED BY THE NMCI DAA. FURTHER DETAILS ON A NMCI FOLLOW-ON CERTIFICATION AND ACCREDITATION PROCESS ARE BEING DEVELOPED AND WILL BE PROVIDED SEPARATELY.
- MUST CHANGE APPLICATION DISTRIBUTION AND NOTIFICATION PROCESSES. FOR AN INTERIM PERIOD, THEY MUST DEVELOP PARALLEL

PROCESSES FOR NMCI AND NON-NMCI SITES. FOR NMCI SITES, APPLICATIONS MUST NOT BE DELIVERED TO SITES WITHOUT FIRST UNDERGOING NMCI CERTIFICATION AND ACCREDITATION.
- MUST STANDARDIZE APPLICATIONS TO REDUCE MULTIPLE VERSIONS. IMPLEMENTATION OF APPLICATIONS ON NMCI SHOULD GREATLY FACILITATE THESE EFFORTS.
- MUST ENSURE DESIGNATED HELP DESK SUPPORT ACTIVITIES ARE WORKING SEAMLESSLY WITH NMCI HELP DESKS. WORKING GROUPS ARE IN THE PROCESS OF DEFINING NMCI AND LEGACY SYSTEM HELP DESK PROCESSES. EACH CDA WILL BE CONTACTED TO PARTICIPATE.
- MUST COMPLETE REQUIRED SSAA DOCUMENTATION FOR ALL APPLICATIONS INTENDED FOR CONTINUED USE ON NMCI. FOR INCREMENT 1.0 AND 1.5 SITES, THE SSAA DOCUMENT IS REQUIRED BY 01 AUGUST 2002. FOR ALL OTHER APPLICATIONS, THE SSAA IS REQUIRED NLT 01 SEPTEMBER 2002.
D. REPORTING: THE PRIMARY TOOL TO ENSURE ACCURATE REPORTING OF LEGACY APPLICATIONS STATUS IS THE NMCI DATABASE. EACH ECHELON II COMMAND WILL TAKE APPROPRIATE ACTION TO ENSURE ALL DATA ELEMENT ENTRIES ARE COMPLETE, ACCURATE, AND MAINTAINED CURRENT FOR THEIR COMMAND AND SUBORDINATE COMMANDS. THIS INCLUDES THE IDENTIFICATION OF EACH APPLICATION'S CDA. THE NMCI PMO WILL CONSOLIDATE THIS DATA FOR WEEKLY REPORTING TO SECNAV AND CNO. REPORTS WILL REFLECT STATUS OF RATIONALIZATION, RFS SUBMISSION, CERTIFICATIONS, ACTION PLANS, AND SSAA DOCUMENTATION.

5. SPECIFIC NAVY POLICY, GUIDANCE AND GOALS WILL BE PROVIDED SHORTLY CONCERNING THE FURTHER REDUCTION OF LEGACY APPLICATIONS AND THE ELIMINATION OF LEGACY NETWORKS REQUIRED TO SUPPORT KIOSKED APPLICATIONS.

6. THIS PROCESS MODIFICATION IS REQUIRED TO FACILITATE THE IMPLEMENTATION AND COMPLETION OF NMCI WITHIN DON. YOUR PERSONAL ATTENTION AND SUPPORT IS REQUESTED TO ENSURE SUCCESS.

7. RELEASED BY VADM R. W. MAYO, USN.//

BT
NNNN

D.2 Navy CNO Message R 301245Z SEP 02

R 301245Z SEP 02 CNO WASHINGTON DC ENTERPRISE STRATEGY FOR MANAGING NMCI APPLICATIONS AND DATABASES

TO CINCLANTFLT NORFOLK VA
CINCPACFLT PEARL HARBOR HI
CINCUSNAVEUR LONDON UK
CINCUSNAVEUR LONDON UK
ASSTSECNAV FM WASHINGTON DC
ASSTSECNAV MRA WASHINGTON DC
ASSTSECNAV RDA WASHINGTON DC
COMUSNAVCENT
COMNAVNETWARCOM NORFOLK VA
COMNAVNETWARCOM NORFOLK VA
NAVWARCOL NEWPORT RI
NAVWARCOL NEWPORT RI
COMNAVSEASYSCOM WASHINGTON DC
OGC WASHINGTON DC
NAVY JAG WASHINGTON DC
NAVY JAG WASHINGTON DC
BUMED WASHINGTON DC
CNET PENSACOLA FL
CNET PENSACOLA FL
BUPERS MILLINGTON TN
BUPERS MILLINGTON TN
COMSC WASHINGTON DC
COMSC WASHINGTON DC
COMNAVAIRSYSCOM PATUXENT RIVER MD
COMNAVAIRSYSCOM PATUXENT RIVER MD
COMNAVSAFECEN NORFOLK VA
COMNAVSAFECEN NORFOLK VA
COMNAVRESFOR NEW ORLEANS LA
COMNAVRESFOR NEW ORLEANS LA
COMNAVLEGSVCCOM WASHINGTON DC
COMNAVLEGSVCCOM WASHINGTON DC
COMNAVSECGRU FT GEORGE G MEADE MD
COMNAVSUPSYSCOM MECHANICSBURG PA

COMNAVSUPSYSCOM DET NORFOLK VA
COMNAVSUPSYSCOM DET NORFOLK VA
NAVSTKAIRWARCEN FALLON NV
CNR ARLINGTON VA
COMSPAWARSYSCOM SAN DIEGO CA
COMSPAWARSYSCOM SAN DIEGO CA
NAVPGSCOL MONTEREY CA
NAVPGSCOL MONTEREY CA
COMNAVFACENGCOM WASHINGTON DC
COMNAVFACENGCOM WASHINGTON DC
COMOPTEVFOR NORFOLK VA
COMOPTEVFOR NORFOLK VA
ONI WASHINGTON DC
COMNAVSPECWARCOM CORONADO CA
DIRSSP WASHINGTON DC
DIRSSP WASHINGTON DC
COMNAVMETOCCOM STENNIS SPACE CENTER MS
COMNAVMETOCCOM STENNIS SPACE CENTER MS
COMNAVSPACECOM DAHLGREN VA
NAVOBSY WASHINGTON DC
NAVOBSY WASHINGTON DC
COMNAVDIST WASHINGTON DC
COMNAVDIST WASHINGTON DC
FLDSUPPACT WASHINGTON DC
NCTSI SAN DIEGO CA
NCTSI SAN DIEGO CA
PEOWTPO CHERRY PT NC
PEOWTPO CHERRY PT NC
PEO CARRIERS WASHINGTON DC
PEO SURFACE STRIKE WASHINGTON DC
PEO EXW WASHINGTON DC
PEO MUW WASHINGTON DC
PEO SUB WASHINGTON DC
PEO THEATER SURFACE COMBATANTS WASHINGTON DC DET B
PEO THEATER SURFACE COMBATANTS WASHINGTON DC DET C
PEO THEATER SURFACE COMBATANTS WASHINGTON DC DET D
PEOASWASM PATUXENT RIVER MD

PEOASWASM PATUXENT RIVER MD
PEOTACAIR PATUXENT RIVER MD
PEOTACAIR PATUXENT RIVER MD
COMNAVNETOPSCOM WASHINGTON DC
COMNAVNETOPSCOM WASHINGTON DC
CHINFO WASHINGTON DC
CNO WASHINGTON DC
INFO SECNAV WASHINGTON DC
UNSECNAV WASHINGTON DC
USCINCPAC HONOLULU HI
USCINCJFCOM NORFOLK VA
CMC WASHINGTON DC
CMC WASHINGTON DC
COMFLTFORCOM NORFOLK VA
COMMARFORLANT
COMMARFORLANT
COMMARFORPAC
COMSECONDFLT
COMTHIRDFLT
COMSIXTHFLT
COMSEVENTHFLT
COMNAVAIRLANT NORFOLK VA
COMNAVAIRPAC SAN DIEGO CA
COMNAVSURFLANT NORFOLK VA
COMNAVSURFPAC SAN DIEGO CA
COMSUBLANT NORFOLK VA
COMSUBPAC PEARL HARBOR HI
MSCLNOLANT NORFOLK VA
MSCLNOLANT NORFOLK VA
MSCLNOPAC PEARL HARBOR HI
COMNAVAIRWARCENWPNDIV CHINA LAKE CA
COMNAVAIRWARCENWPNDIV CHINA LAKE CA
NAVAIRSYSCOM CHERRY PT NC
NAVFACENGCOMDET NFI PORT HUENEME CA
NAVSURFWARCENDIV DAHLGREN VA
NAVSURFWARCENDIV DAHLGREN VA
NAVICP PHILADELPHIA PA

COMMARFORRES
COMMARCORMATCOM ALBANY GA
COMMARCORMATCOM ALBANY GA
COMNAVCRUITCOM MILLINGTON TN
COMNAVCRUITCOM MILLINGTON TN
COMMARCORSYSCOM QUANTICO VA
COMMARCORSYSCOM QUANTICO VA
FLTINFOWARCEN NORFOLK VA
FLTINFOWARCEN NORFOLK VA
NCTF-CND WASHINGTON DC
NRL WASHINGTON DC
NRL WASHINGTON DC
PEOSTRKWPNSUAVN PATUXENT RIVER MD
PEOSTRKWPNSUAVN PATUXENT RIVER MD
DON CIO WASHINGTON DC
PEO IT WASHINGTON DC
PEO IT WASHINGTON DC
MITNOC QUANTICO VA
MITNOC QUANTICO VA
NAVMEDINFOMGMTCEN BETHESDA MD

ADMINISTRATIVE MESSAGE
ROUTINE
UNCLAS
MSGID/GENADMIN/CNO WASHINGTON DC N6N7/006-02//
SUBJ/ENTERPRISE STRATEGY FOR MANAGING NMCI APPLICATIONS AND DATABASES //
REF/A/GENADMIN/CNO WSHINGTON DC/252250ZFEB2002/001-02//
NARR/REF A IS NAVY INFORMATION OFFICER MESSAGE DIRECTING ECHELON II COMMANDERS TO IMPLEMENT PROCESSES TO REDUCE APPLICATIONS AND DATABASES WITHIN THEIR COMMANDS USING THE ISF TOOLS DATABASE.// POC/TRAVERSO, TIMOTHY/-/CNO NIO/-/TEL:703-604-7806//
AMPN/EMAIL: TRAVERSO.TIMOTHY@HQ.NAVY.MIL//
POC/STICINSKI, RON/CAPT/NADTF/-/TEL:202-764-2942//
AMPN/EMAIL: RON.STICINSKI@NAVY.MIL//
POC/CORMAN, CYNTHIA/-/NADTF/-/TEL:202-764-0852//
AMPN/EMAIL: CYNTHIA.CORMAN@NAVY.MIL//
POC/HEDIN, TED/-/NADTF/-/TEL:202-764-0012//

AMPN/EMAIL: HEDINW@NCTC.NAVY.MIL//
POC/KELLY, JUDY/LCDR/NADTF/-/TEL:202-764-1813//
AMPN/EMAIL: JUDY.KELLY@NAVY.MIL//
RMKS/1. THIS IS A COMBINED DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER (DON CIO), NAVY INFORMATION OFFICER (NIO) AND DIRECTOR, NMCI MESSAGE.
2. THE REDUCTION AND CONSOLIDATION OF NAVY APPLICATIONS AND DATABASES TO THE ABSOLUTE MINIMUM REQUIRED TO SUPPORT THE NAVY'S MISSION IS THE PRIMARY GOAL. COORDINATING THE EFFORTS OF FUNCTIONAL AREA MANAGERS (FAMS), ECHELON II COMMANDS, NAVY APPLICATION AND DATABASE TASK FORCE (NADTF), NETWARCOM (NMCI DESIGNATED APPROVAL AUTHORITY (DAA)), TASK FORCE WEB (TFW), AND THE ENTERPRISE RESOURCE PLANNING (ERP) PILOTS, WITHOUT IMPACTING NMCI SEAT ROLLOUT, REQUIRES A COMMON OPERATIONAL PICTURE OF THE NAVY'S APPLICATIONS AND DATABASES. CURRENTLY THE FOLLOWING CONDITIONS EXIST: A. THE ISF TOOLS DATABASE IS THE AUTHORITATIVE DATABASE FOR NAVY APPLICATIONS ON NMCI AND IT IS THE TOOL FOR EVERY NAVY COMMAND TO ENSURE OPERATIONALLY REQUIRED APPLICATIONS ARE ORDERED FOR NMCI IMPLEMENTATION. B. THE DEPARTMENT OF THE NAVY (DON) APPLICATION AND DATABASE MANAGEMENT SYSTEM (DADMS) HAS ACHIEVED INITIAL OPERATIONAL CAPABILITY. DADMS WILL BE THE SINGLE AUTHORITATIVE DATABASE FOR ALL APPLICATIONS AND DATABASES, WILL CONTAIN A COMPLETE INVENTORY OF ALL AUTHORIZED APPLICATIONS AND DATABASES RESIDING ON ALL NAVY NETWORKS (E.G. NMCI, IT21 AND OCONUS BLII) AND WILL SERVE AS A TOOL TO IDENTIFY AND TRACK QUARANTINED APPLICATIONS. THIS MESSAGE DIRECTS ACTION TO ACHIEVE COMMON OPERATIONAL PICTURE OF THE NAVY'S APPLICATIONS AND DATABASES IN DADMS AND THE CONTINUED USE OF THE ISF TOOLS DATABASE AS THE PRIMARY TOOL FOR ORDERING AND IMPLEMENTING APPLICATIONS IN NMCI. THIS MESSAGE DIRECTS ALL ECHELON II COMMANDS TO ENSURE THEIR FINAL RATIONALIZED LIST OF ALL NMCI APPLICATIONS (AT HEADQUARTERS AND ALL SUBORDINATE COMMANDS) IS REFLECTED IN THE ISF TOOLS DATABASE WITHIN SIXTY DAYS OF THE DATE TIME GROUP OF THIS MESSAGE, REQUIRES THE APPROVAL OF THE APPLICABLE FAM AND NIO FOR THE SUBSEQUENT ADDITION OF APPLICATIONS TO ISF TOOLS DATABASE BY ECHELON II COMMANDS AND SUBORDINATE COMMANDS, MANDATES THAT EVERY NAVY APPLICATION WILL HAVE A DESIGNATED CENTRAL DESIGN ACTIVITY AND/OR OWNER IDENTIFIED BY NAME WITH CONTACT INFORMATION IAW PARA 4 OF REF A, AND SPECIFIES A PROCESS TO BE FOLLOWED TO TRACK ALL QUARANTINED APPLICATIONS.

3. REQUIRED ACTION AND THE ASSOCIATED TIME LINE IS POSTED
AT HTTPS:"FWD DOUBLE SLASH"WWW.DADMS.NAVY.MIL UNDER THE "POLICY AND
GUIDANCE" LINK.//
BT
#0179
NNNN

D.3 Navy CNO Message COSPAWARSYSCOM/PMW164 242225Z MAY 02

Subject: 242225Z MAY 02 - COSPAWARSYSCOM/PMW164 - NMCI PROCESS SUMMIT AGRE EMENTS//

Follow Up Flag: Follow up
Flag Status: Flagged

Prec: ROUTINE

DTG: 242225Z MAY 02

From:

To:

Info: SECNAV WASHINGTON DC
DON CIO WASHINGTON DC
CNO WASHINGTON DC
CINCLANTFLT NORFOLK VA
CINCPACFLT PEARL HARBOR HI
CINCUSNAVEUR LONDON UK
COMUSNAVCENT
COMNAVSEASYSCOM WASHINGTON DC
COMNAVAIRSYSCOM PATUXENT RIVER MD
COMNAVAIRLANT NORFOLK VA
COMNAVAIRPAC SAN DIEGO CA
COMNAVSURFPAC SAN DIEGO CA
COMNAVSURFLANT NORFOLK VA
PEO IT WASHINGTON DC
COMNAVDIST WASHINGTON DC
COMNAVLEGSVCCOM WASHINGTON DC
COMNAVSAFECEN NORFOLK VA
COMOPTEVFOR NORFOLK VA
DIRSSP WASHINGTON DC
FLDSUPPACT WASHINGTON DC
NAVHISTCEN WASHINGTON DC
NAVOBSY WASHINGTON DC
NAVPGSCOL MONTEREY CA
NAVSTKAIRWARCEN FALLON NV
NCTSI SAN DIEGO CA
USNA ANNAPOLIS MD
BUMED WASHINGTON DC
PEO CARRIERS WASHINGTON DC
PEO SURFACE STRIKE WASHINGTON DC

PEO IT DET SAN DIEGO CA
PEO EXW WASHINGTON DC
PEO MUW WASHINGTON DC
PEO SUB WASHINGTON DC
PEO THEATER SURFACE COMBATANTS WASHINGTON DC DET B
PEO THEATER SURFACE COMBATANTS WASHINGTON DC DET C
PEO THEATER SURFACE COMBATANTS WASHINGTON DC DET D
PEOASWASM PATUXENT RIVER MD
PEOTACAIR PATUXENT RIVER MD
PEOTACAIR PMA TWO THREE ONE DET NORTH ISLAND CA
NCTF-CND WASHINGTON DC
COMNAVFACENGCOM WASHINGTON DC
COMNAVMETOCCOM STENNIS SPACE CENTER MS
COMNAVSECGRU FT GEORGE G MEADE MD
COMNAVSPACECOM DAHLGREN VA
COMNAVSPECWARCOM CORONADO CA
COMNAVSUPSYSCOM MECHANICSBURG PA
CNET PENSACOLA FL
DISA WASHINGTON DC
COMNAVNETOPSCOM WASHINGTON DC
COMNAVRESFOR NEW ORLEANS LA
COMNAVPERSCOM MILLINGTON TN
CTF-NMCI WASHINGTON DC
SPAWARSYSCEN NORFOLK DET SAN DIEGO CA
SPAWARSYSCEN SAN DIEGO CA
NRL WASHINGTON DC
SPAWARSYSCEN CHARLESTON SC
COMSC WASHINGTON DC
ONI WASHINGTON DC
PRESINSURV NORFOLK VA
PEOSTRKWPNSUAVN PATUXENT RIVER MD
PEOSTRKWPNSUAVN DET WPC WASHINGTON DC
PEOWTPO CHERRY PT NC
PEOTACAIR PMA TWO SEVEN TWO DET JACKSONVILLE FL
COMMARFORRES
COMMARFORLANT
CG MCCDC QUANTICO VA
COMMARCORMATCOM ALBANY GA
MITNOC QUANTICO VA
COMMARFORPAC
CG MCRC QUANTICO VA
CG TECOM QUANTICO VA
CMC WASHINGTON DC
COMMARCORSYSCOM QUANTICO VA
NAVWARCOL NEWPORT RI
SPAWARSYSCEN NORFOLK VA

ASSTSECNAV RDA WASHINGTON DC

Subj: NMCI PROCESS SUMMIT AGREEMENTS//

UNCLAS //N2060//

MSGID/GENADMIN/COMSPAWARSYSCOM/PMW164//

SUBJ/NMCI PROCESS SUMMIT AGREEMENTS//

REF/A/GENADMIN/PEO IT WASHINGTON DC/202304ZMAY2002//

AMPN/REF A IS NMCI 20K ROLLOUT EXECUTION ORDER.//
POC/ROBERT LOGAN/COL/NMCI DEPUTY DIRECTOR/-/TEL:CML:(703)685-5510
/EMAIL:RLOGAN'AT'SPAWAR.NAVY.MIL//
POC/CRAIG MADSEN/CAPT/NAVY NMCI PM/-/TEL:(619)524-7553
/EMAIL:EMAIL: MADSENC'AT'SPAWAR.NAVY.MIL//
POC/RICH GLOVER/CIV/PM USMC NMCI/-/TEL:DSN:278-0709
/EMAIL:EMAIL: GOVERRA'AT'MCSC.USMC.MIL//
POC/TIM TRAVERSO/CIV/NADTF-NAVY CIO/-/TEL:(703)602-5995
/EMAIL:EMAIL: TRAVERSO.TIMOTHY'AT'HQ.NAVY.MIL//

RMKS/1. THIS IS A COORDINATED NAVAL MESSAGE FROM DIRECTOR NMCI, NAVY AND MARINE CORPS PROGRAM OFFICES, AND THE NMCI ISF. ON MAY 7 - 9, REPRESENTATIVES FROM THESE ORGANIZATIONS HELD A SUMMIT TO DISCUSSAND DEFINE PROCESSES TO IMPROVE AND ACCELERATE NEAR TERM NMCI SEATROLLOUT. THIS NAVAL MESSAGE SUMMARIZES THE AGREEMENTS REACHED ON THESE PROCESSES.

2. BACKGROUND. FUTURE NMCI CUSTOMERS HAVE SEEN A VARIETY OF PROCESS DOCUMENTS, HAVE ATTENDED VARIOUS NMCI FORUMS, OR HAVE HAD THE OPPORTUNITY TO OBSERVE THE EARLY NMCI INSTALLATION EFFORTS. TO DATE, NMCI SEAT ROLLOUT HAS BEEN SLOWER THAN EXPECTED OR DESIRED. THROUGH A COMBINED EFFORT AT THE NMCI PROCESS SUMMIT, HIGH LEVERAGE ITEMS WERE IDENTIFIED RELATED TO LEGACY APPLICATIONS AND INFORMATION ASSURANCE. ALSO, RELATED NMCI TRANSITION ISSUES WERE IDENTIFIED AND PRIORITIZED.

3. PROCESS CHANGES. THE DIRECTOR NMCI AUTHORIZES THE PROCESSES SUMMARIZED BELOW FOR IMMEDIATE IMPLEMENTATION AT SITES TRANSITIONING TO NMCI IN ACCORDANCE WITH REF A. SPECIFIC PROCESS DETAILS WILL BE PROVIDED SEPCOR, BUT THE SIGNIFICANT CHANGES ARE SUMMARIZED BELOW.

A. LEGACY APPLICATIONS:
(1) LOCAL APPLICATION LOADING (EITHER MANUALLY OR THROUGH AN IMAGE BUILD) IS APPROVED. APPLICATIONS SUITABLE FOR LOCAL LOADING MUST BE ON THE SITE'S RATIONALIZED LIST.
(2) USER TO APPLICATION MAPPING WILL BE REQUIRED AT THE TIME FINAL RATIONALIZED LISTS ARE DUE (AOR-60 DAYS).
(3) REVISE LEGACY APPLICATION PROCESSES TO SHORTEN TIMELINE BY APPLYING APPLICATION "FUNNELING" PROCESSES AND EMPOWERING THE NADTF TO APPLY APPLICATION RULE SETS TO REDUCE RATIONALIZED LISTS. ON-SITE LEADERSHIP WILL EXPLAIN THE FUNNELING PROCESS IN DETAIL. ITS PURPOSE IS TO QUICKLY SORT AND PRIORITIZE EXISTING LEGACY APPLICATIONS.
(4) THE LEGACY APPLICATION MIGRATION RULE SET (LED BY NADTF) INCLUDES THE FOLLOWING:
(A) WINDOWS 2000 COMPLIANT APPLICATIONS ONLY
(B) COMPLIANT WITH DON/DOD SECURITY POLICY
(C) NO PERSONAL, NON-MISSION, OR NON-BUSINESS-RELATED SOFTWARE
(D) NO GAMES
(E) NO FREEWARE OR SHAREWARE
(F) NO BETA OR TEST VERSION SOFTWARE PACKAGES
(G) NO APPLICATION DEVELOPMENT SOFTWARE (EXCEPTION APPLIES FOR APPROVED SCIENCE AND TECHNOLOGY [S&T] SEATS)
(H) NO AGENTS
(I) NO DUPLICATION OF STANDARD SEAT SERVICES
(J) NO 8 OR 16 BIT APPLICATIONS
(5) ALL MEDIA NEEDS TO BE HELD ONSITE AND SUBMITTED TO THE ISF. CONTINUE TO USE THE ISF TOOLS DB TO CREATE REQUEST FOR SERVICE (RFS) FOR ALL LEGACY APPLICATIONS REQUIREMENTS.
(6) IA VULNERABILITY ASSESSMENT PACKAGES WILL BE DEVELOPED AND PROVIDED POST SEAT CUTOVER VICE PRIOR TO SEAT CUTOVER.
(7) APPLICATIONS WILL BE TESTED USING A PIAB, A LADRA TEST SEAT, OR THE ISF CERTIFICATION LAB IN SAN DIEGO. ISF WILL DETERMINE MEANS AND LOCATION OF TESTING.
(8)APPLICATIONS THAT SUCCESSFULLY PASS NMCI CERTIFICATION AND B1/B2 TESTING WILL BE AUTHORIZED FOR OPERATION ON NMCI.
(9)ISF WILL GENERATE A WEEKLY REPORT FOR DELIVERY TO THE NMCI DAA. THE WEEKLY REPORT WILL PROVIDE INFORMATION PERTAINING TO APPLICATION INSTALLATION METHOD, TESTING RESULTS, AND NUMBER OF SEATS INSTALLED FOR EACH SITE.
(10) APPLICATIONS THAT FAIL CERTIFICATION AND/OR B1/B2 TESTING WILL BE QUARANTINED ON THE LEGACY NETWORK.
(11) APPLICATIONS THAT ARE IDENTIFIED, SUBMITTED, OR APPROVED LATE WILL BE QUARANTINED ON THE LEGACY NETWORK.
B. INFORMATION ASSURANCE: THE FOLLOWING ISSUES HAVE RECEIVED PROGRAM ENDORSEMENT AND HAVE BEEN FORWARDED TO THE NMCI DAA FOR APPROVAL.

(1) SHORTEN TIMELINE TO ACHIEVE SITE IATO FROM 31 DAYS TO 24 DAYS INCLUDING 8 DAYS FOR FORMAL DAA REVIEW AND APPROVAL. DAA TO ASSIGN DELEGATE AUTHORITY TO ASSIST IN OVERCOMING DAA AVAILABILITY. ISF/PMO TO PROVIDE DAA 24-72 HOUR NOTICE OF UPCOMING CRITICAL DECISION MILESTONES.
(2) IATO/IATC IN PARALLEL. GOVERNMENT APPROVAL TO LAUNCH APPLICATIONS TO TEST SEATS ON THE OPERATIONAL NETWORK FOR TESTING. APPROVAL EXTENDS TO APPLICATIONS AND SEATS USED FOR NMCI SECURITY/GPO TESTING ONLY. APPLICATIONS INCLUDE ONLY THOSE CURRENTLY RUNNING IN LEGACY ENVIRONMENT.
(3) ON COMPLETION OF BOUNDARY 2 BUILD AND SCAN, DAA TO APPROVE, IN PHONECON OR EMAIL VICE LETTER, CONNECTION TO NETWORK.
(4) ON COMPLETION OF SERVER FARM BUILD AND SCAN, DAA TO APPROVE, IN PHONE CON OR EMAIL VICE LETTER, APPROVAL TO CONNECT TO BOUNDARY.

4. WORKING ISSUES. IN ADDITION TO THE LEGACY APPLICATION AND INFORMATION ASSURANCE PROCESS CHANGES OUTLINED ABOVE, WORK CONTINUES ON COMMAND AND CONTROL AT SITES, THE ROLLOUT SCHEDULE BEYOND THE FIRST 20K SEATS, AN ENTERPRISE POLICY/PLAN TO BASELINE THE KIOSK PROCESS, AND THE USER TO APP MAPPING PROCESS. APPROXIMATELY 50 TRANSITION ISSUES WERE IDENTIFIED AS HAVING THE POTENTIAL TO DIRECTLY EFFECT RAPID SEAT ROLLOUT AND WILL ALSO CONTINUE TO BE WORKED. EXAMPLES OF THESE ISSUES INCLUDE MACS, S&T CLIN 0038, LEGACY DEVICE SUPPORT, AND END USER AVAILABILITY.

5. THE NMCI DIRECTOR'S OFFICE, NAVY AND MARINE CORPS PROGRAM OFFICES, AND THE ISF WILL CONTINUE TO REFINE PROCESSES TO INCORPORATE LESSONS LEARNED AS SEAT ROLLOUT CONTINUES. YOUR CONTINUED INVOLVEMENT AND COMMENTS ARE BOTH SPECIFICALLY REQUESTED
AND APPRECIATED.//

BT
#5456
NNNN

D.4 Navy CNO 120155Z JUN 02

Subject: 120155Z JUN 02 - CNO - NAVY STANDARD APPLICATIONS//

Importance: Low

Follow Up Flag: Follow up
Flag Status: Flagged

R 120155Z JUN 02 CNO WASHINGTON DC NAVY STANDARD APPLICATIONS//

TO CINCLANTFLT NORFOLK VA
CINCPACFLT PEARL HARBOR HI
CINCUSNAVEUR LONDON UK
CINCUSNAVEUR LONDON UK
ASSTSECNAV FM WASHINGTON DC
ASSTSECNAV FM WASHINGTON DC
ASSTSECNAV MRA WASHINGTON DC
ASSTSECNAV MRA WASHINGTON DC
ASSTSECNAV RDA WASHINGTON DC
ASSTSECNAV RDA WASHINGTON DC
COMUSNAVCENT
NAVWARCOL NEWPORT RI
NAVWARCOL NEWPORT RI
COMNAVSEASYSCOM WASHINGTON DC
OGC WASHINGTON DC
OGC WASHINGTON DC
NAVY JAG WASHINGTON DC
NAVY JAG WASHINGTON DC
BUMED WASHINGTON DC
BUMED WASHINGTON DC
CNET PENSACOLA FL
CNET PENSACOLA FL
BUPERS MILLINGTON TN
BUPERS MILLINGTON TN
COMSC WASHINGTON DC
COMSC WASHINGTON DC
COMNAVAIRSYSCOM PATUXENT RIVER MD
COMNAVAIRSYSCOM PATUXENT RIVER MD
COMNAVSAFECEN NORFOLK VA
COMNAVSAFECEN NORFOLK VA
COMNAVRESFOR NEW ORLEANS LA
COMNAVRESFOR NEW ORLEANS LA
COMNAVLEGSVCCOM WASHINGTON DC
COMNAVLEGSVCCOM WASHINGTON DC
COMNAVSECGRU FT GEORGE G MEADE MD

COMNAVMETOCCOM STENNIS SPACE CENTER MS

COMNAVSUPSYSCOM MECHANICSBURG PA
COMNAVSUPSYSCOM DET NORFOLK VA
COMNAVSUPSYSCOM DET NORFOLK VA
NAVSTKAIRWARCEN FALLON NV
CNR ARLINGTON VA
COMSPAWARSYSCOM SAN DIEGO CA
COMSPAWARSYSCOM SAN DIEGO CA
NAVPGSCOL MONTEREY CA
NAVPGSCOL MONTEREY CA
COMNAVFACENGCOM WASHINGTON DC
COMNAVFACENGCOM WASHINGTON DC
COMOPTEVFOR NORFOLK VA
COMOPTEVFOR NORFOLK VA
ONI WASHINGTON DC
COMNAVSPECWARCOM CORONADO CA

INFO SECNAV WASHINGTON DC
UNSECNAV WASHINGTON DC
DIRSSP WASHINGTON DC
DIRSSP WASHINGTON DC
COMNAVMETOCCOM STENNIS SPACE CENTER MS
COMNAVSPACECOM DAHLGREN VA
NAVOBSY WASHINGTON DC
NAVOBSY WASHINGTON DC
COMNAVDIST WASHINGTON DC
COMNAVDIST WASHINGTON DC
FLDSUPPACT WASHINGTON DC
FLDSUPPACT WASHINGTON DC
NCTSI SAN DIEGO CA
NCTSI SAN DIEGO CA
PEOWTPO CHERRY PT NC
PEOWTPO CHERRY PT NC
PEO CARRIERS WASHINGTON DC
PEO SURFACE STRIKE WASHINGTON DC
PEO EXW WASHINGTON DC
PEO MUW WASHINGTON DC
PEO SUB WASHINGTON DC
PEO THEATER SURFACE COMBATANTS WASHINGTON DC DET B
PEO THEATER SURFACE COMBATANTS WASHINGTON DC DET C
PEO THEATER SURFACE COMBATANTS WASHINGTON DC DET D
PEOASWASM PATUXENT RIVER MD
PEOASWASM PATUXENT RIVER MD
PEOTACAIR PATUXENT RIVER MD
PEOTACAIR PATUXENT RIVER MD
COMNAVNETOPSCOM WASHINGTON DC
COMNAVNETOPSCOM WASHINGTON DC

USCINCPAC HONOLULU HI
USCINCJFCOM NORFOLK VA
CMC WASHINGTON DC
CMC WASHINGTON DC
COMFLTFORCOM NORFOLK VA
COMMARFORLANT
COMMARFORLANT
COMMARFORPAC
COMSECONDFLT
COMTHIRDFLT
COMSIXTHFLT
COMSEVENTHFLT
COMNAVAIRLANT NORFOLK VA
COMNAVAIRPAC SAN DIEGO CA
COMNAVSURFLANT NORFOLK VA
COMNAVSURFPAC SAN DIEGO CA
COMSUBLANT NORFOLK VA
COMSUBPAC PEARL HARBOR HI
MSCLNOLANT NORFOLK VA
MSCLNOLANT NORFOLK VA
MSCLNOPAC PEARL HARBOR HI
COMNAVAIRWARCENWPNDIV CHINA LAKE CA
COMNAVAIRWARCENWPNDIV CHINA LAKE CA
NAVAIRSYSCOM CHERRY PT NC
NAVFACENGCOM DET NFI PORT HUENEME CA
NAVSURFWARCENDIV DAHLGREN VA
NAVSURFWARCENDIV DAHLGREN VA
NAVICP PHILADELPHIA PA
COMMARFORRES
COMMARCORMATCOM ALBANY GA
COMMARCORMATCOM ALBANY GA
COMNAVCRUITCOM MILLINGTON TN
COMNAVCRUITCOM MILLINGTON TN
COMMARCORSYSCOM QUANTICO VA
COMMARCORSYSCOM QUANTICO VA
NCTF-CND WASHINGTON DC
NRL WASHINGTON DC
NRL WASHINGTON DC
PEOSTRKWPNSUAVN PATUXENT RIVER MD
PEOSTRKWPNSUAVN PATUXENT RIVER MD
DON CIO WASHINGTON DC
DON CIO WASHINGTON DC
PEO IT WASHINGTON DC
PEO IT WASHINGTON DC
MITNOC QUANTICO VA
MITNOC QUANTICO VA

NAVMEDINFOMGMTCEN BETHESDA MD

ADMINISTRATIVE MESSAGE

ROUTINE

UNCLAS
4630

MSGID/GENADMIN/CNO N09T/005-02//

SUBJ/NAVY STANDARD APPLICATIONS//

REF/A/MSG/CNO WASHINGTON DC/012017ZMAR2002//

REF/B/MSG/CNO WASHINGTON DC/252250ZFEB2002//

NARR/REF A IS NAVY INFORMATION OFFICER MESSAGE (CNO N09T 002-02) ESTABLISHING STANDARD APPLICATIONS TO BE USED ON NAVY NETWORKS. REF
B IS NAVY INFORMATION OFFICER MESSAGE (CNO N09T 001-02) ON NMCI LEGACY APPLICATIONS TRANSITION PROCESS.//
POC/ALAND, DAVID/CAPT/CNO OPNAV N6K/LOC:WASHINGTON DC.
/EMAIL:(703) 604-6880 ALAND.DAVID(AT)HQ.NAVY.MIL//

RMKS/1. THIS MESSAGE IS A JOINT NAVY INFORMATION OFFICER AND DIRECTOR NMCI MESSAGE AND DIRECTLY SUPPORTS THE IMPLEMENTATION OF NMCI, INTEROPERABILITY BETWEEN NAVY NETWORKS AND USERS AND STANDARDIZATION OF COMMERCIAL OFF THE SHELF (COTS) AND GOVERNMENT OFF THE SHELF (GOTS) APPLICATIONS IN THE NAVY.

2. THIS MESSAGE CANCELS REF A AND PROVIDES ADDITIONAL MANDATORY DIRECTION FOR COTS APPLICATION REDUCTION THAT SHOULD BE APPLIED IMMEDIATELY TO ALL NAVY NETWORKS (E.G. NMCI, IT21 AND OCONUS BLII). SPECIFICALLY, THE APPLICATIONS AND ASSOCIATED VERSIONS LISTED IN PARAGRAPHS 3.A AND 4.A BELOW REPRESENT THE NAVY'S PREFERRED APPLICATIONS FOR ALL NAVY NETWORKS BASED UPON WIDE SPREAD USE THROUGH-OUT THE NAVY AND/OR OPERATIONAL REQUIREMENTS AS SPECIFIED BY FUNCTIONAL AREA MANAGERS. SOME NAVY NETWORKS MAY REQUIRE DIFFERENT COTS APPLICATIONS THAT PERFORM THE SAME OR SIMILAR FUNCTIONS OR A DIFFERENT VERSION OF THE APPLICATION LISTED. FOR THOSE COTS APPLICATIONS, FOLLOW THE EXCEPTION GUIDANCE LISTED BELOW IN PARAGRAPH 3.B OR 4.C. AS TECHNOLOGY ADVANCES AND APPLICATIONS ARE REVISED, THE NMCI PROVIDED BASIC SEAT SERVICES (PARAGRAPH 3.A) AND THE OTHER COTS AND GOTS APPLICATIONS (PARAGRAPH 4.A) WILL BE UPDATED

TO REFLECT THOSE ADVANCES AND REVISIONS AS SPECIFIED BY THE APPLICABLE FUNCTIONAL AREA MANAGER.

3. EACH ECHELON II COMMAND SHALL ESTABLISH APPLICATION AND APPLICATION VERSION CONTROL AS SOON AS POSSIBLE ON THE FOLLOWING STANDARDIZED APPLICATIONS BEING PROVIDED AS NMCI BASIC SEAT SERVICES FOR THE INDICATED COTS APPLICATIONS. UNLESS OTHERWISE APPROVED BY THE NAVY INFORMATION OFFICER, ECHELON II COMMANDS WILL ELIMINATE ANY UNNECESSARILY DUPLICATIVE APPLICATION FROM THEIR RATIONALIZED LIST:

A. COTS FUNCTION	APPLICATION/VERSION
OPERATING SUITE	MICROSOFT WINDOWS 2000 BUILD 2195 SP1
OFFICE SUITE	MICROSOFT OFFICE PRO 2000 SR-1A
WORD PROCESSING	MICROSOFT WORD 2000 9.0.3821 SR1
DESKTOP DATABASE	MICROSOFT ACCESS 2000 9.0.3821 SR-1
PRESENTATIONS	MICROSOFT POWER POINT 2000 9.0.5519
SPREADSHEETS	MICROSOFT EXCEL 2000 9.0.3821 SR1
EMAIL CLIENT	MICROSOFT OUTLOOK 2000 9.0.0.3821
CALENDAR	MICROSOFT OUTLOOK 2000 9.0.0.3821
INTERNET BROWSER	MICROSOFT INTERNET EXPLORER 5.5 SP-1 128 BIT
INTERNET BROWSER	COMMUNICATOR 4.76 (NETSCAPE)
VIRUS PROTECTION	NORTON A/V CORP EDITION V7.51 (SYMANTEC)
PDF VIEWER	ACROBAT READER V.4.05D (ADOBE)
TERMINAL EMULATOR	REFLECTION 8.0.5 (WRQ) HOST (TN3270,VT100, X-TERMINAL)
COMPRESSION TOOL	WINZIP V.8 (WINZIP)
COLLABORATION TOOL	NET MEETING V3.01 (4.4.3385)
MULTIMEDIA	REAL PLAYER 8 (REAL NETWORKS)
MULTIMEDIA	WINDOWS MEDIA PLAYER V7.0.0.1956
WEB CONTROLS	MACROMEDIA SHOCKWAVE V 8.0 (MACROMEDIA)
WEB CONTROLS	FLASH PLAYER 5.0 (MACROMEDIA)
WEB CONTROLS	APPLE QUICKTIME MOVIE AND AUDIO VIEWER V4.12 (APPLE)
WEB CONTROLS	IPIX V6.2.0.5 (INTERNET PICTURES)
SECURITY	INTRUDER ALERT V3.6 (AXTENT)
SECURITY	ESM V5.1 (AXTENT)
SOFTWARE MGMT	RADIA CLIENT CONNECT (NOVADIGM)
INVENTORY, REMOTE CONTROL	TIVOLI TMA 3.7 (IBM/TIVOLI)
DIAL-UP CONNECTIVITY	PAL (MCI/WORLDCOM)
VPN	VPN CLIENT (ALCATEL)

B. IF AN ECHELON II COMMANDER REQUIRES AN ADDITIONAL VERSION OF A COTS APPLICATION PROVIDED BY NMCI BASIC SEAT SERVICES (PARAGRAPH 3.A) OR OTHER COTS APPLICATIONS PERFORMING THE SAME FUNCTION, THE

ECHELON II COMMANDER MUST REQUEST AN EXCEPTION SEPARATELY FROM BOTH THE NAVY INFORMATION OFFICER AND THE APPLICABLE FUNCTIONAL AREA MANAGER. ANY EXCEPTION REQUEST SHOULD INCLUDE THE NUMBER OF LICENSES HELD FOR EACH VERSION, THE NUMBER OF ACTUAL USERS OF EACH VERSION, THE PLAN FOR MIGRATING TO THE CORRESPONDING APPLICATION PROVIDED BY THE NMCI BASIC SEAT SERVICES AND JUSTIFICATION FOR INCLUDING THE APPLICATION FOR TRANSITION TO NMCI, OR RETAINING THE APPLICATION FOR USE ON IT21 OR OCONUS BLII NETWORKS (INCLUDE THE UNIQUE FUNCTION BEING PERFORMED BY THIS OTHER APPLICATION AND WHY IT IS OPERATIONALLY REQUIRED).

4. EACH ECHELON II COMMAND SHALL ESTABLISH APPLICATION AND APPLICATION VERSION CONTROL AS SOON AS POSSIBLE ON THE FOLLOWING ADDITIONAL STANDARDIZED COTS AND GOTS APPLICATIONS. ECHELON II COMMANDS WILL UPDATE APPLICATION VERSIONS ON THEIR RATIONALIZED LIST IN THE INFORMATION STRIKE FORCE (ISF) TOOLS DATABASE TO REFLECT THE VERSIONS LISTED BELOW:

A. SOFTWARE FUNCTION	APPLICATION/VERSION
ALCOHOL AND DRUG MANAGEMENT	ADMITS: VERSION 2.0
AUTOMATED TRAVEL ORDER SYSTEM	ATOS: VERSION 040-05.04.05 OR 5.4.5
AIRCRAFT WEIGHT AND BALANCE	AWBS: VERSION 8.1 (VERSION 9.1 WHEN CERTIFIED)
AVIATION MAINTENANCE MANAGEMENT	AV3M: VERSION 004-14.00.00
CAREER INFORMATION	CIPM 99: VERSION 1.0D-5
MAINTENANCE AUDITING SYSTEM	CSEC: VERSION 1.1 (VERSION 2H, 2K WHEN CERTIFIED)
DEFENSE REQUISITIONING SYSTEM	DAMES: VERSION 2.11.046
DEFENSE PROPERTY ACCOUNTING SYSTEM	DPAS: VERSION 15.0.14 (MYEUREKA VERSION 6.1.313 AND SUPRA NT VERSION 36038.0)
PLAIN LANGUAGE ADDRESS SYSTEM	DPVS: VERSION 6.0
PERSONNEL SECURITY	EPSQ VERSION: 2.2 (SUBJECT EDITION AND SECURITY OFFICER EDITION)
HAZMAT MANAGEMENT	HMIS: VERSION DEC2001 (INCLUDING FIRST EDITION HMIRS, VERSION TBD)
READINESS MANAGEMENT	IRRS: VERSION 2.0.1
TRAVEL MANAGEMENT	JFTR: VERSION 4.2 (FOLIO VIEWER)
LOGISTICS MANAGEMENT	FEDLOG: VERSION 5.1
FITNESS REPORT PREPARATION	NAVFIT98: VERSION 2.002.0021
DRUG SCREENING SYSTEM	NDSP: VERSION 5.0
ELECTRONIC TRAINING SYSTEM	NEETS: VERSION 1.0
MAINTENANCE READINESS MANAGEMENT	RMSWIN: VERSION 8.0
AVIATION REPORTING	SHARP: VERSION 4.0.3 SR1
MEDICAL MANAGEMENT	SAMS: VERSION 25.08.02.00

NAVAL MESSAGE PREPARATION .....TURBOPREP VERSION 2.02A-5N
(INCLUDING TURBOPREP PATCH A)
B. COGNIZANT DESIGN ACTIVITIES SHOULD ENSURE THAT THE MOST RECENT VERSION/UPDATE IS RELEASED TO SITES AS QUICKLY AS POSSIBLE. ALL REQUIREMENTS PROMULGATED IN REF B MUST BE MET PRIOR TO RELEASE.
C. IF AN ECHELON II COMMANDER REQUIRES AN ADDITIONAL VERSION OF AN APPLICATION LISTED IN PARA 4.A OR OTHER APPLICATIONS PERFORMING THE SAME FUNCTION, THE ECHELON II COMMANDER MUST REQUEST THIS EXCEPTION SEPARATELY FROM BOTH THE NAVY INFORMATION OFFICER AND APPLICABLE FUNCTIONAL AREA MANAGER. ANY EXCEPTION REQUEST SHOULD INCLUDE THE NUMBER OF LICENSES HELD FOR EACH VERSION, THE NUMBER OF ACTUAL USERS OF EACH VERSION, THE PLAN FOR MIGRATING TO THE CORRESPONDING APPLICATION LISTED IN PARAGRAPH 4.A AND JUSTIFICATION FOR INCLUDING THE APPLICATION FOR TRANSITION TO NMCI OR RETAINING THE APPLICATION FOR USE ON IT21 OR OCONUS BLII NETWORKS (INCLUDE THE UNIQUE FUNCTION BEING PERFORMED BY THIS OTHER APPLICATION AND WHY IT IS OPERATIONALLY REQUIRED).

5. THIS MESSAGE WILL BE UPDATED TO REFLECT THOSE CHANGES IDENTIFIED BY FUNCTIONAL AREA MANAGERS AS THEY DEVELOP THEIR RESPECTIVE APPLICATION AND DATABASE PORTFOLIOS.//

BT
#0309
NNNN

D.5 Navy CNO 031345Z AUG 01

Subject: [6R00050818U.CGS] NMCI LEGACY APPLICATIONS//
RAAUZYUW RUENAAA0503 2151344-UUUU--RUEASUU.
ZNR UUUUU

R 031345Z AUG 01 ZYB ZYW
FM CNO WASHINGTON DC//N09T//
TO CINCPACFLT PEARL HARBOR HI//00/N6//
CINCLANTFLT NORFOLK VA//00/N6//
NAVWARCOL NEWPORT RI//00//
COMNAVSEASYSCOM WASHINGTON DC//00/03/05//
USNA ANNAPOLIS MD//00//
BUMED WASHINGTON DC//00/CIO//
CNET PENSACOLA FL//00/N6//
BUPERS MILLINGTON TN//00/01EE/014//
COMSC WASHINGTON DC//00/N6//
COMNAVAIRSYSCOM PATUXENT RIVER MD//00/CIO//
COMUSNAVCENT//00/N6/N65/N65B//
COMNAVSAFECEN NORFOLK VA//00//
COMNAVAIRLANT NORFOLK VA//00/06//
COMNAVAIRPAC SAN DIEGO CA//00/06//
COMNAVSURFLANT NORFOLK VA//00/06//
COMNAVSURFPAC SAN DIEGO CA//00/06//
COMNAVRESFOR NEW ORLEANS LA//00/N6/N62//
COMNAVLEGSVCCOM WASHINGTON DC//00//
COMNAVSECGRU FT GEORGE G MEADE MD//00/N6//
COMNAVSUPSYSCOM MECHANICSBURG PA//00/N6//
NAVSTKAIRWARCEN FALLON NV//00//
CNR ARLINGTON VA//00//
COMSPAWARSYSCOM SAN DIEGO CA//00/PD16/PMW164/CIO//
NAVPGSCOL MONTEREY CA//00//
COMNAVCRUITCOM MILLINGTON TN//00//
COMNAVFACENGCOM WASHINGTON DC//00/63//
COMOPTEVFOR NORFOLK VA//00//
ONI WASHINGTON DC//00/N6//
COMNAVSPECWARCOM CORONADO CA//00/N6//
CHINFO WASHINGTON DC//00//
DIRSSP WASHINGTON DC//00/N6//
COMNAVMETOCCOM STENNIS SPACE CENTER MS//00/N6//
COMNAVSPACECOM DAHLGREN VA//00/N6//
NAVOBSY WASHINGTON DC//00//
COMNAVDIST WASHINGTON DC//00//
COMNAVLEGSVCCOM WASHINGTON DC//00/06//
COMOPTEVFOR NORFOLK VA//00//
FLDSUPPACT WASHINGTON DC//00//

NCTSI SAN DIEGO CA//00//
PEOWTPO CHERRY PT NC//00//
PEO CARRIERS WASHINGTON DC//00//
PEO SURFACE STRIKE WASHINGTON DC//00//
PEO EXW WASHINGTON DC//00//
PEO MUW WASHINGTON DC//00//
PEO SUB WASHINGTON DC//00//
PEO THEATER SURFACE COMBATANTS WASHINGTON DC DET B //00//
PEO THEATER SURFACE COMBATANTS WASHINGTON DC DET C //00//
PEO THEATER SURFACE COMBATANTS WASHINGTON DC DET D //00//
PEOASWASM PATUXENT RIVER MD//00//
PEOTACAIR PATUXENT RIVER MD//00//
COMNAVNETOPSCOM WASHINGTON DC//00/N6/N3//
NCTF-CND WASHINGTON DC//00/31//
NRL WASHINGTON DC//00/5500/5540/5544//
PEOSTRKWPNSUAVN PATUXENT RIVER MD//00//
INFO SECNAV WASHINGTON DC//AAUSN//
UNSECNAV WASHINGTON DC//JJJ//
USCINCPAC HONOLULU HI//J6//
CMC WASHINGTON DC//ALS/C4/I&L/P&R/M&RA/PP&O/AVN/IPS//
COMMARFORLANT//G6//
ASSTSECNAV RDA WASHINGTON DC//JJJ//
COMMARFORRES//G6//
COMMARCORMATCOM ALBANY GA//G6//
COMMARCORSYSCOM QUANTICO VA//C4/ISR/SEI//
DON CIO WASHINGTON DC//00//
PEO IT WASHINGTON DC//00//
MITNOC QUANTICO VA//OPS//
NAVMEDINFOMGMTCEN BETHESDA MD//42//
COMMARFORPAC//G6//
BT
UNCLAS

MSGID/GENADMIN/CNO N09T/005-01//

SUBJ/NMCI LEGACY APPLICATIONS//

REF/A/DOC/DON CIO/YMD:20010423//
REF/B/GENADMIN/CNO WASHINGTON DC/061414ZJUL2001/09T//
REF/C/GENADMIN/PEO IT WASHINGTON DC/282200ZFEB2001//
REF/D/DOC/SPAWARSYSCOM/13JUL2001//

NARR/REF A IS DON CIO POLICY MEMO CALLING FOR DEPARTMENT-WIDE REDUCTION OF LEGACY APPLICATIONS. REF B IS NAVY CIO MESSAGE 003-01 THAT PROVIDES GUIDANCE FOR NMCI TRANSITION OF LEGACY APPLICATIONS. REF C IS PEO IT MESSAGE THAT PROVIDES AN OVERVIEW OF

THE PROCESS AND PROCEDURES TO SUPPORT THE ACCESS OF LEGACY APPLICATIONS UNDER NMCI. REF D IS THE NMCI LEGACY APPLICATIONS TRANSITION GUIDE VERSION 2.0.//

POC/ALAND, DAVID/CAPT/OPNAV NAVY CIO/-/TEL:703-604-6880// AMPN/EMAIL: ALAND.DAVID@HQ.NAVY.MIL//

POC/LAWAETZ,ALLIE/CIV/PEO IT/-/TEL:703-601-4750// AMPN/EMAIL:LAWAETZA@SPAWAR.NAVY.MIL//

RMKS/1. THIS IS NAVY CIO MESSAGE 005/01 WHICH PROVIDES MANDATORY REQUIREMENTS FOR NMCI LEGACY APPLICATIONS TRANSITION, AMPLIFYING REFS A THRU D. LESSONS LEARNED SHOW THAT LEGACY APPLICATION CERTIFICATION IS THE CRITICAL PATH FOR NMCI TRANSITION. WE HAVE MORE COTS AND GOTS APPLICATIONS CURRENTLY IN USE THAN IS EITHER EFFICIENT OR AFFORDABLE. NMCI TRANSITION OFFERS AN OPPORTUNITY TO PROFOUNDLY IMPROVE THIS, BUT REQUIRES IMMEDIATE ACTION. ECHELON II COMMANDERS ARE EACH RESPONSIBLE FOR THE IDENTIFICATION, RATIONALIZATION, AND SUBMISSION FOR CERTIFICATION OF APPLICATIONS, VIA A PROCESS THAT INCLUDES INTEGRATION, CONSOLIDATION, AND ELIMINATION OF APPLICATIONS AND DATABASES. INDIVIDUAL SITE COMMANDERS ARE RESPONSIBLE FOR MEETING PRESCRIBED DEADLINES AND GOALS IN SUPPORT OF THEIR ECHELON II COMMANDERS.

2. ACTION:

A. ALL ECHELON II COMMANDERS MUST SUBMIT A REPORT, INCLUDING AN INITIAL APPLICATION INVENTORY, IAW REF A. A REPORT TEMPLATE WILL BE PROVIDED SEPARATELY. IOT SUPPORT NMCI SCHEDULES, THIS REPORT IS NOW REQUIRED NLT 01OCT01.

B. REFS B THRU D DETAIL THE TRANSITION PROCESS FOR LEGACY APPLICATIONS TO NMCI, AND IS AMPLIFIED BELOW. WAIVERS TO THESE REQUIREMENTS WILL BE AT THE DISCRETION OF THE NAVY CIO, OPNAV 09T.

(1) 120 DAYS PRIOR TO ASSUMPTION OF RESPONSIBILITY (AOR) BY THE INFORMATION STRIKE FORCE (ISF), COMMENCE THE TRANSITION PROCESS TO INCLUDE VALIDATION OF THE SITE APPLICATION INVENTORY. PRIOR TO THIS, INITIAL RATIONALIZATION AGAINST MISSION REQUIREMENTS AND COMMON BUSINESS RULES (PROVIDED SEPARATELY) AND PRESURVEY QUESTIONNAIRES (PSQ'S) MUST BE COMPLETED. DELIVERY TO ISF OF THIS RATIONALIZED LIST OF APPLICATIONS SHOULD ALSO COMMENCE.

(2) 60 DAYS PRIOR TO AOR DELIVER THE COMPLETED LIST OF ALL COTS AND GOTS APPLICATIONS THAT WILL BE REQUIRED TO OPERATE ON NMCI. 50 PERCENT OF ALL GOTS APPS MUST BE DELIVERED TO THE ISF CERTIFICATION LABORATORY AND ACCEPTED.

(3) 45 DAYS PRIOR TO AOR, 75 PERCENT OF IDENTIFIED APPLICATIONS (COTS AND GOTS) SHOULD BE DELIVERED AND ACCEPTED FOR CERTIFICATION.

(4) 30 DAYS PRIOR TO AOR ALL REMAINING IDENTIFIED APPLICATIONS (COTS AND GOTS) MUST BE SUBMITTED AND ACCEPTED FOR CERTIFICATION. APPLICATIONS NOT SUBMITTED BY THIS DEADLINE WILL NOT TRANSITION TO NMCI AT THE SCHEDULED CUTOVER DATE.

(5) ALL FIRST INCREMENT SITES THAT HAVE NOT DELIVERED THEIR SURVEYS/INVENTORIES AND APPLICATIONS MUST COMPLETE AND DELIVER THEM WITHIN 30 DAYS FROM RECEIPT OF THIS MESSAGE.

(6) SOME SECOND INCREMENT SITES WITH AOR IN OCT/NOV 01 ARE ALREADY WITHIN THE 120 AND/OR 60 DAY DEADLINES. FOR THESE SITES, INVENTORY MUST BEGIN IMMEDIATELY, AND RATIONALIZED LISTS ARE DUE NO LATER THAN SCHEDULED AOR DATE. ALL APPLICATIONS MUST BE PROVIDED TO ISF AND ACCEPTED NO LATER THAN 30 DAYS AFTER AOR.

3. THE NMCI LEGACY APPLICATIONS TRANSITION PROCESS PROVIDES ECHELON II COMMANDS THE OPPORTUNITY TO ACHIEVE DISCIPLINE IN THEIR IT APPLICATIONS ENVIRONMENT. SOME COMMANDS ARE ALREADY SUCCEEDING AT THIS AND HAVE REALIZED SUBSTANTIAL LEGACY APPLICATION REDUCTIONS. PROACTIVE PARTICIPATION AND COLLABORATION WITH THE ISF IS ESSENTIAL. COMMANDERS ARE ACCOUNTABLE FOR THE SUCCESSFUL OPERATIONAL TRANSITION OF THEIR COMMANDS AND COMPLIANCE WITH THE PROCEDURES OUTLINED IN THIS MESSAGE AND REFS A THRU D. SPECIFIC COMMAND AOR SCHEDULES ARE AVAILABLE AT [QUOTE] WWW.EDS.COM/NMCI/TRANSITION.HTM [UNQUOTE] ALL LOWER CASE.
4. I WILL BE INDIVIDUALLY CONTACTING EVERY ECHELON II COMMANDER IN THE NEXT WEEK TO EMPHASIZE THE IMPORTANCE OF THIS MESSAGE. YOUR PERSONAL FEEDBACK IS ENCOURAGED AT ANY TIME. RELEASED BY VADM R.W. MAYO, NAVY CIO.//
BT
#0503
NNNN

Appendix E — NMCI Application (NADTF) Ruleset (Revised)

Version 2.94 dtd 31 January 2003

Ruleset Is A Reference	The NMCI Ruleset is designed to be a summary of the information contained in the Legacy Applications Transition Guide (LATG) and the NMCI Release Development and Deployment Guide (NRDDG). Should questions arise from the use of the Ruleset, the user should refer to the LATG, NRDDG or contact the Navy Applications Data Base Task Force (NADTF) for clarification.

RULESET NUMBER	RULE NAME	RULE DESCRIPTION	OWNER REQUIRED ACTION	STATUS
RULE 1	**Windows 2000 (W2K) Compatible**	The candidate application is not compatible with the Windows 2000 operating system. This means it will either not run properly under Windows 2000 or that it interferes with the normal functionality of the operating system.	NAVY IO (NADTF) will not consider waivers of this Ruleset. Claimant must resolve the incompatibility by working with the application POR/CDA and owning FAM to upgrade the application to Windows 2000 compatibility or it should be replaced by another that is Windows 2000 compliant. Once compliant version is identified it will be submitted for NMCI testing and certification. Applications that cannot be corrected will be Quarantined for no more than 6 months and then be removed from the quarantine workstation. The application will then be removed from the rationalized list and archived in the ISF Tools database. Echelon II Commands will cancel the RFS and unlink the application from their UICs in the ISF Tools database.	**FAIL**
RULE 2	**NMCI Group Policy Object (GPO) Compatible**	The candidate application is not compatible with the Group Policy Object (GPO) security rules for the workstation. For instance, if the candidate application requires full control of the c:\winnt folder in order to run, this violates NMCI enterprise policy governing connection to the NMCI network.	NAVY IO (NADTF) will not consider waivers of this Ruleset. Claimant must resolve the incompatibility by working with the application POR/CDA, owning FAM, ISF, IATT, and NMCI DAA in correcting the GPO failure. IATT or ISF will provide the technical data detailing cause of the failure. Once the GPO failure is resolved, the application will be re-tested. GPO Policy changes may be requested from the NMCI DAA. Applications that cannot be corrected will be Quarantined for no more than 6 months and then be removed from the quarantine workstation. If the application cannot be corrected, then the application must be removed from the rationalized list and archived in the ISF Tools database. Echelon II Commands will cancel RFS and unlink this application to their UICs in the ISF Tools database.	**FAIL**

RULESET NUMBER	RULE NAME	RULE DESCRIPTION	OWNER REQUIRED ACTION	STATUS
RULE 3	No Duplication of Gold Disk Software or Services	The candidate application or service duplicates the functionality of the NMCI Standard Seat Services ("Gold Disk") application. (Example: Word 2000 replaces all versions of WordPerfect and other word processors. Windows Media Player, Real Player, and QuickTime replace all other audio/video players).	Claimant should discard the current application and use the application or service that exists on the Gold Disk. This application is not eligible for quarantine. Waiver requests may be submitted to NAVY IO (NADTF), but approvals will only be given if Claimant can show degradation to the mission, and can show they cannot afford to upgrade to authorized NMCI software or services. If the waiver is not approved or if no waiver is submitted, the application must be removed from the rationalized list and archived in the ISF Tools database. Echelon II Commands will cancel RFS and unlink this application to their UICs in the ISF Tools database	KILL UNLESS WAIVER AUTHORIZED (NRFC)
RULE 4	Comply with DON/NMCI Boundary 1 and 2 Policies	The ISF or IATT have determined, through testing, that the candidate application is non-compliant with NMCI Boundary firewall policies (violation of B1/B2 Rulesets).	Claimant must resolve violation with the IATT, application POR/CDA, owning FAM, ISF, and NMCI DAA to determine how to correct the Boundary policy violation. Once the policy violation is resolved, the application will be re-tested. NAVY IO (NADTF) will not consider waivers of this Ruleset. Requests to operate a non-compliant system for B1 Firewall policy violations are managed by OPNAV and B2 policy changes are reviewed and managed by the NMCI DAA. B2 boundary issues may be resolved by moving servers into NMCI enclave. Applications that cannot be corrected will be Quarantined for no more than 6 months and then be removed from the quarantine workstation. These applications will then be removed from the rationalized list and archived in the ISF Tools database. Echelon II Commands will cancel RFS and unlink this application to their UICs in the ISF Tools database.	FAIL
RULE 5	No Setup, Installation, Uninstallation, Update and Auto update Tools or Utilities	The candidate application is actually a tool or utility used to load and remove application. Since ISF conducts all application installation and removal in NMCI, these types of files will not be authorized in ISF Tools DB or on the Rationalized List. Examples include Setup, Install, Uninstall, Launch, Autolaunch, Run, AutoRun, Updater, AutoUpdater or other installation type Applications	ISF will not test this application and NAVY IO (NADTF) will not consider waivers. These types of applications will be removed from tracking and the Legacy Applications Rationalized List and archived in the ISF Tools database. It will not be installed on a quarantine workstation. Echelon II Commands will cancel RFS and unlink this application to their UICs in the ISF Tools database.	KILL (NRFC)

RULESET NUMBER	RULE NAME	RULE DESCRIPTION	OWNER REQUIRED ACTION	STATUS
RULE 6	No Games	The candidate application is a "game" as defined by PEO-IT, NAVY IO and the PMO and is prohibited on the NMCI environment.	ISF will not test this application unless the POR/CDA, Echelon II and/or FAM determine the game is required for mission accomplishment (Modeling, Simulation, or Training). The Claimant must submit a waiver request to Navy IO (NADTF). Applications already approved by the M&S and/or Training FAM will not require waivers. If the waiver is not approved or if no waiver is submitted, the application must be removed from the Legacy Applications Rationalized List and archived in the ISF Tools database. It will not be installed on a quarantine workstation. Echelon II Commands will cancel RFS and unlink this application to their UICs in the ISF Tools database.	KILL UNLESS WAIVER AUTHORIZED (NRFC)
RULE 7	No Freeware or Shareware	The candidate application is "Freeware" or "Shareware" as defined by PEO-IT, NAVY IO or the PMO and is prohibited in the NMCI environment. Enterprise life cycle support and licensing issues accompany most "Freeware".	Waivers for shareware will not be considered. Waivers for freeware will require an Echelon II, POR/CDA or FAM to generate a waiver request to NADTF. The waiver should include a request for the appropriate FAM to endorse the CDA, and will identify the CDA's willingness to support the application across the NMCI Enterprise. The NADTF will coordinate the waiver request with the NMCI DAA. Life cycle support and licensing issues for freeware must be resolved before they can be distributed to the Navy Enterprise. This application will not be installed on a quarantine workstation. If the waiver is not approved or if no waiver is submitted, the application must be removed from the Legacy Applications Rationalized List and archived in the ISF Tools database. The Echelon II Commands will cancel RFS and unlink this application to their UICs in the ISF Tools database.	KILL UNLESS WAIVER AUTHORIZED (NRFC)
RULE 8	No Beta/Test Software (Authorized on S&T Seats Only)	The candidate application is a "beta" or a "test" version, as defined by the PEO-IT, NAVY IO, or the PMO and is therefore prohibited in the NMCI environment.	ISF will not test this application and the Navy IO (NADTF) will not consider waivers. These types of applications will not be tracked through the Legacy Application Transition process. These applications are not entered into the ISF Tools Database, not included on any rationalized list, nor should an RFS be submitted. If the Beta or Test Software is critical for mission accomplishment, the Claimant may purchase an S&T Seat. This application will not be installed on a quarantine workstation. Echelon II Commands will cancel RFS and unlink this application to their UICs in the ISF Tools database.	KILL (NRFC)

RULESET NUMBER	RULE NAME	RULE DESCRIPTION	OWNER REQUIRED ACTION	STATUS
RULE 9	No Application Development Software (Authorized on S&T Seats Only)	The candidate application is "application development" software, as defined by PEO-IT, NAVY IO-or the PMO, and therefore is not authorized on standard NMCI Seats. The candidate application would be permitted if operated on an NMCI ordered Science and Technology (S&T) Seat. Simple Application Development Software will not be tracked on the Rationalized List in the ISF Tools Database nor submitted for certification. Complex Application Development Software will require full NMCI testing and certification and will be tracked on the Rationalized List in the ISF Tools Database.	Simple Application Development Software will not be tested by ISF and the Navy IO (NADTF) will not consider waivers. These types of applications will not be tracked through-the Legacy Application Transition process. These applications are not entered into the ISF Tools Database, not included on any rationalized list, nor should an RFS be submitted. If the application development software is critical for mission accomplishment, the Claimant may purchase an S&T Seat, which allows for the installation of development software. This application will not be installed on a quarantine workstation. Echelon II Commands will cancel RFS and unlink this application to their UICs in the ISF Tools database. Complex Application Development Software will be tested, certified, and deployed by the ISF and will be tracked on the Rationalized List in the ISF Tools Database and will have an RFS submitted.	KILL (NRFC)
RULE 10	No Agent Software	The candidate application is "agent" software, as defined by PEO-IT, NAVY IO or the PMO. Agents in the NMCI environment are controlled by ISF. No other candidate agents are allowed in the NMCI environment. Agents are code modules installed on client machines (or network devices) often used to poll, monitor, and collect system or network node performance data and send it to management consoles elsewhere on the network. These present a security risk to NMCI. Network monitoring and management are the responsibilities of the ISF.	These types of applications will be removed from tracking in the Legacy Applications Rationalized List and the ISF Tools Database. NADTF will Kill these applications and waivers will not be considered. No polling and monitoring of legacy networks and systems and collecting of data is authorized from within NMCI Polling, monitoring and collecting system and network data of legacy networks and systems is still authorized from legacy network assets only. Viewing collected legacy network or system data from NMCI seats is allowed using non-agent software.	KILL (NRFC)

RULESET NUMBER	RULE NAME	RULE DESCRIPTION	OWNER REQUIRED ACTION	STATUS
RULE 11	**Gold Disk Compatible**	The application software is not compatible with the standard "Gold Disk" software and services. This means that the candidate application does not interact properly with one or more of the set of applications or services that have been selected to be installed on all NMCI seats.	NAVY IO (NADTF) will not consider waivers of this Ruleset. The application is Quarantined for no more than 6 months and then it is removed from the quarantine workstation. The application will be removed from the rationalized list and archived in the ISF Tools database. Echelon II Commands will cancel the RFS and unlink this application to their UICs in the ISF Tools database. Claimants and POR/CDA must work with the ISF to determine Gold Disk compatibility issues. The POR/CDA then works with the owning FAM to upgrade, replace or retire the application. Once a compliant version is identified it must be submitted for NMCI testing.	**FAIL**
RULE 12	**No Peripherals, Peripheral Drivers or Internal Hardware**	The candidate submission is a component (driver or hardware helper app) dealing directly with allowing a peripheral piece of hardware to function (Scanner, Printer, Plotters, Chartmakers, CDRW drive, ZIP or JAZ drive, Camcorder, PDA, etc). This enabling software must be tracked with the hardware on the Peripherals list and not entered into ISF Tools Database or listed on the Rationalized List. Internal hardware and the associated driver are not permitted within NMCI.	Peripherals and enabling software (drivers) are not entered into the ISF Tools Database nor placed on the Rationalized List. Peripherals and Peripheral Drivers are tracked separately from the ISF Tools Database and the Rationalized List, and are included in the Peripheral Drivers List. The Peripherals Drivers List is submitted to the ISF on-site for processing. If the driver is part of a bundled software package, that bundled package is handled like an application. The bundled package is entered into the ISF Tools Database, placed on the Rationalized List, and tested by the ISF.	**KILL (NRFC)**
RULE 13	**No personal, non-mission, or non-business related software**	The candidate application is “personal, non-mission, or non-business related”, and is therefore prohibited in the NMCI environment.	ISF will not test this application unless the POR/CDA, Echelon II and/or FAM determine that this application is required for mission accomplishment. These applications will not be installed on a quarantine workstation. The claimant must submit a waiver request to Navy IO (NADTF). If the waiver is not approved or submitted, the application must be removed from the rationalized list and archived in the ISF Tools database. Echelon II Commands will cancel RFS and unlink this application to their UICs in the ISF Tools database.	**KILL UNLESS WAIVER AUTHORIZED (NRFC)**

RULESET NUMBER	RULE NAME	RULE DESCRIPTION	OWNER REQUIRED ACTION	STATUS
RULE 14	**8/16-Bit Applications**	8-bit and 16-bit applications may migrate into the NMCI environment with an approved NAVY IO (NADTF) waiver, and a realistic migration plan that identifies a path to 32-bit status. Applications without approved waivers will not migrate to NMCI or Quarantined environments. Identification of an application as 8-bit or 16-bit does not stop the testing process (PIAB and LADRA). The application must pass all other rules and testing for 8-bit and 16-bit waivers to be approved.	Claimant and/or POR/CDA will submit a waiver immediately to NAVY IO (NADTF) requesting the 8/16-bit application migrate into NMCI. The request must include a detailed migration plan to get 8/16-bit application to 32-bit status. ISF must process and certify the application while the waiver is being submitted. ISF will hold the deployment of the application until waiver is authorized. If the waiver is not authorized (disapproved), the application is Quarantined for no more than 6 months, then removed from the quarantine workstation and archived in the ISF Tools database. Applications for which a waiver was not submitted, will not be Quarantined, will be removed from the rationalized list and archived in the ISF Tools database. Echelon II Commands will cancel RFS and unlink this application to their UICs in the ISF Tools database.	**PROCESS AND CERTIFY APPLICATION - HOLD FOR DEPLOYMENT UNTIL WAIVER AUTHORIZED**

Definitions	
Fail	Fail is defined as an application that violates the NMCI Application Ruleset by failing to successfully meet compliance or usability testing standards. These applications are flagged as Quarantined and will operate on a Quarantined workstation in the legacy environment until the Ruleset violation or test failure is resolved or a waiver to operate within NMCI has been submitted and approved.
Kill	Kill is defined as an application that violates the NMCI Application Ruleset. The application is not compliant with the rules and standards for applications within NMCI as set by the Navy IO. These applications will not be flagged as Quarantine and will be removed from the Rationalization List and ISF Tools database, unless a waiver to the rule is submitted and approved.
NRFC (Not Recommended For Certification)	NRFC is used by the ISF to designate any application that violates the NMCI Application Ruleset and will likely result in a Kill designation when reviewed by NADTF. Applications with an NRFC status have not been packaged or tested in the NMCI environment. This is an application that has not been processed by the ISF for violation of one or more of the following Rulesets: 3 – Duplication of Gold Disk 5 – No Setup Executables 6 - No Games 7 – No Freeware/Shareware 8 – No Beta Software 9 – No Development Software 10 – No Agent Software 12 – No Peripherals or Peripheral drivers 13 – No personal, non-mission, non-business software.
Application Development Software	Any software that generates or allows the user to create programming code which compiles into executable (.exe) files that are installed and can be run from the user's workstation. Application Development Software is only permitted to reside on S&T seats.
Agent Software	Any software that polls, monitors and/or captures network traffic or queries network nodes for the purpose of reporting the captured information back to the user or another network node. This type of information is considered sensitive and its capture and dissemination poses a security risk.

Appendix F — Classified Legacy Applications Transition Process

1.0 — CNO GUIDANCE

This document represents a complete baseline overview of the Classified Legacy Applications Transition Process. It is intended for Navy Marine Corps Intranet (NMCI) customers involved in the transition of Classified Legacy Applications. Both Information Strike Force (ISF) and Government program management personnel have worked in close cooperation to design the processes and procedures described here. All CNO guidance, Naval messages, and requirements addressed in the Legacy Applications Rapid Certification Phase, section 1.0, apply in the processing of Classified Legacy Applications.

2.0 — OVERALL LEGACY APPLICATIONS TRANSITION PROCESS

An overview of the NMCI Legacy Applications Transition Process is provided in the Legacy Applications Rapid Certification Phase, Section 4.0. The classified legacy applications process does not differ significantly from the processing of unclassified applications in the LA Rapid Certification Phase, except where stated below.

The Certification Phase includes Assumption of Responsibility (AOR), Seat Cutover (start), and Seat Cutover (end). The Risk Mitigation Phase begins when Seat Cutover is complete and continues until transition is complete. These distinct and comprehensive processes contain the main pieces of information crucial to transition success and are explained in greater detail in the main sections of this guide. Within the Classified Legacy Applications Transition Process, customers will become involved with:

- The creation of a Classified Rationalized List of applications
- The submission of Classified Requests for Service (CRFSs) and application media to ISF.
- Functional Testing of the application
- Assisting the ISF with IA Compliance Assessment

Within the Risk Mitigation Phase, information regarding system documentation, transition planning, and accreditation will be required. This guide does not address the Risk Mitigation Phase.

Figure F-1 depicts an overview of the legacy application transition. It shows the distinction between the Rapid Certification and Risk Mitigation Phases. Again, this process does not differ significantly from the processing of classified legacy applications. It breaks down the Rapid Certification Phase into smaller processes that describe the "life of a transitioning application." Each of these smaller processes, the information needed for each, and the key people involved with each, are covered in the main sections of this guide.

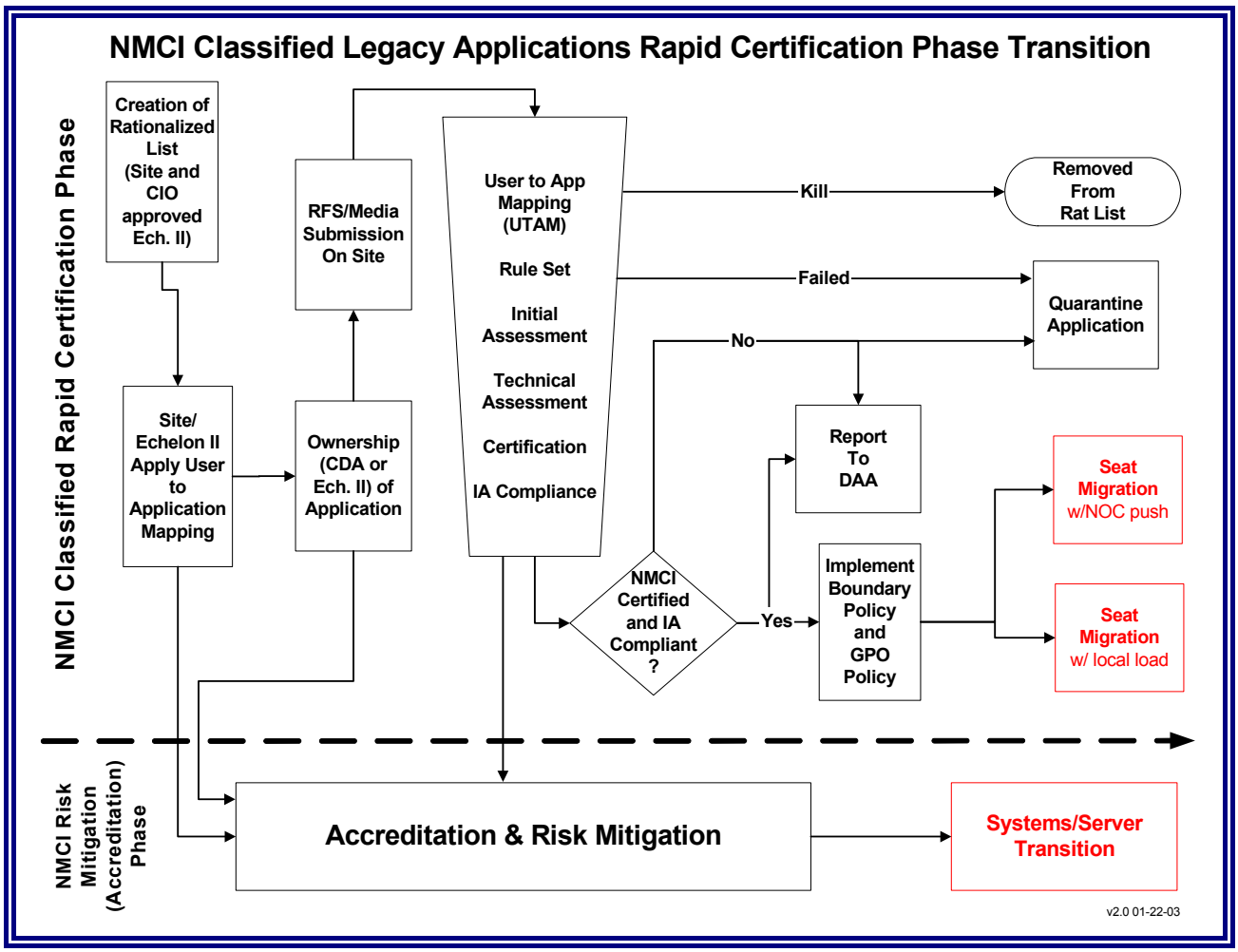


Figure F-1. NMCI Classified Legacy Applications Rapid Certification Phase Transition

3.0 —CLASSIFIED LEGACY APPLICATIONS TRANSITION PROCESS (RAPID CERTIFICATION PHASE)

Figure F-2 depicts the detailed Classified Legacy Applications Transition Process from start to finish. Notice the legend at the bottom right side of Figure F-2. The colors in the legend correspond to ownership of primary responsibility for completion of the process. For example, the "Media Submission" box is blue, and represents a Government/site responsibility for completion. Note that many of the processes are tan, indicating a joint responsibility for completion shared by the ISF and the Government.

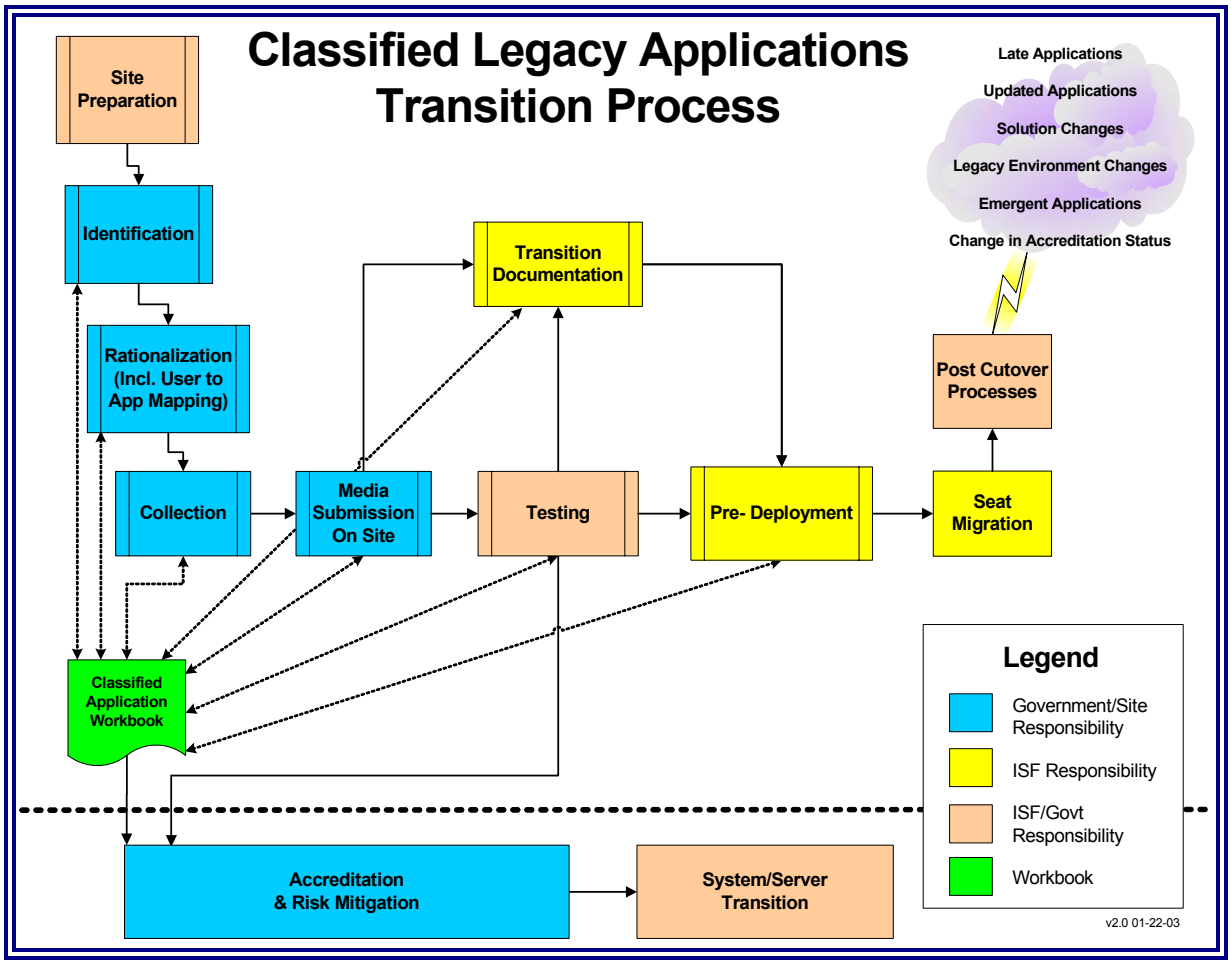


Figure F-2. Classified Legacy Applications Transition Process

The use of the ISF Tools Database is the main difference between the processing of unclassified and classified legacy applications. The Unclassified Rapid Certification Phase (for unclassified legacy applications) utilizes the ISF Tools Database, while the Classified Legacy Applications Transition Process maintains manual tracking of the Classified Legacy Applications Rationalized Lists, Workbooks, and CRFSs.

The overall goal of the Rapid Certification Phase and the Classified Legacy Applications Transition Process is to work with the ISF to ensure the right applications are available to the NMCI seats of the right people at the right time, to ensure completion of the mission and business of the DON. From the customer's perspective, this means many things, including:

- Understanding who uses particular applications at the site.
- Understanding what version(s) of an application are in use at the site.
- Communicating with ISF and Program Management Office (PMO) personnel to help them understand the applications.
- Communicating with appropriate Echelon II personnel as lists of needed applications are reviewed.

- Making the resources available to accomplish the processes.

3.1 Classified Site Preparation

Figure F-3 depicts the details of site preparation from the NMCI customer perspective. The activities are designed to get a site ready to start the transition process well before any contractor or government program management personnel are involved. The major difference here is the requirement for a secure facility/storage, custody, and personnel clearances. This is the vital piece in the whole Classified Legacy Applications transition process and its importance cannot be overstated. To that end, the site Information System Security Manager/Officer (ISSM/O) is the one individual uniquely placed to ensure that all site security requirements and arrangements are carefully planned and coordinated well in advance of the arrival of any ISF transitioning teams. In association with the LAPOC the Command/Site ISSM/O, Site DAA, and ISF SM will ensure that the following areas are properly addressed and coordinated:

- Obtain secured classified storage for classified documentation
- Obtain secure classified workspace for classified application processing
- Acquire CRFS from EDS NMCI website or this Appendix
- Determine facility requirements for Classified PIAB or Classified Legacy Application Deployment Readiness Activity (CLADRA) seat configuration
- Acquire local SIPRNET Interim Authority to Connect (IATC) for CPIAB
- Review, Accept and Assign facilities

Customers should contact the Site Transition Execution Manager (STEM) Management Office (SMO) at the Navy NMCI PMO, SPAWAR PMW-164 for specific questions on Classified Legacy Application transition issues. The E-mail address for the SMO is legacyap@spawar.navy.mil

Customers must plan for the best location at their site for a secure test area to place a Classified Point of Presence (PoP)-In-A-Box (CPIAB) or NMCI Test Seat. The CPIAB is a “mini-NMCI environment” used by the ISF to understand application characteristics. The NMCI Test Seat is an actual NMCI seat used when the Classified NMCI base infrastructure is in place.

This is important because it gives ISF and Information Assurance (IA) personnel a way to understand the ports and protocols that applications use when they communicate. Deployment of a CPIAB or Classified NMCI Test Seat to a site comes later in the transition process, but a wise site prepares facilities and, among other things, makes network access arrangements, and understands power requirements in advance of its arrival. Further information on the CPIAB and Classified NMCI Test Seat can be obtained by contacting the ISF Site Manager (SM) and Site Solutions Engineering Team.

Once the preparatory steps have been completed, the site goes to the Identification and Rationalization processes.

3.2 Classified Application Identification and Rationalization

Once again the major differences between the Unclassified Legacy Application Transition process and the Classified Legacy Applications Transition Process are the use of manual submission and tracking methods of the:

- Classified Legacy Applications Rationalized List
- The Classified Legacy Applications Workbook
- The CRFS
- Certification Letter

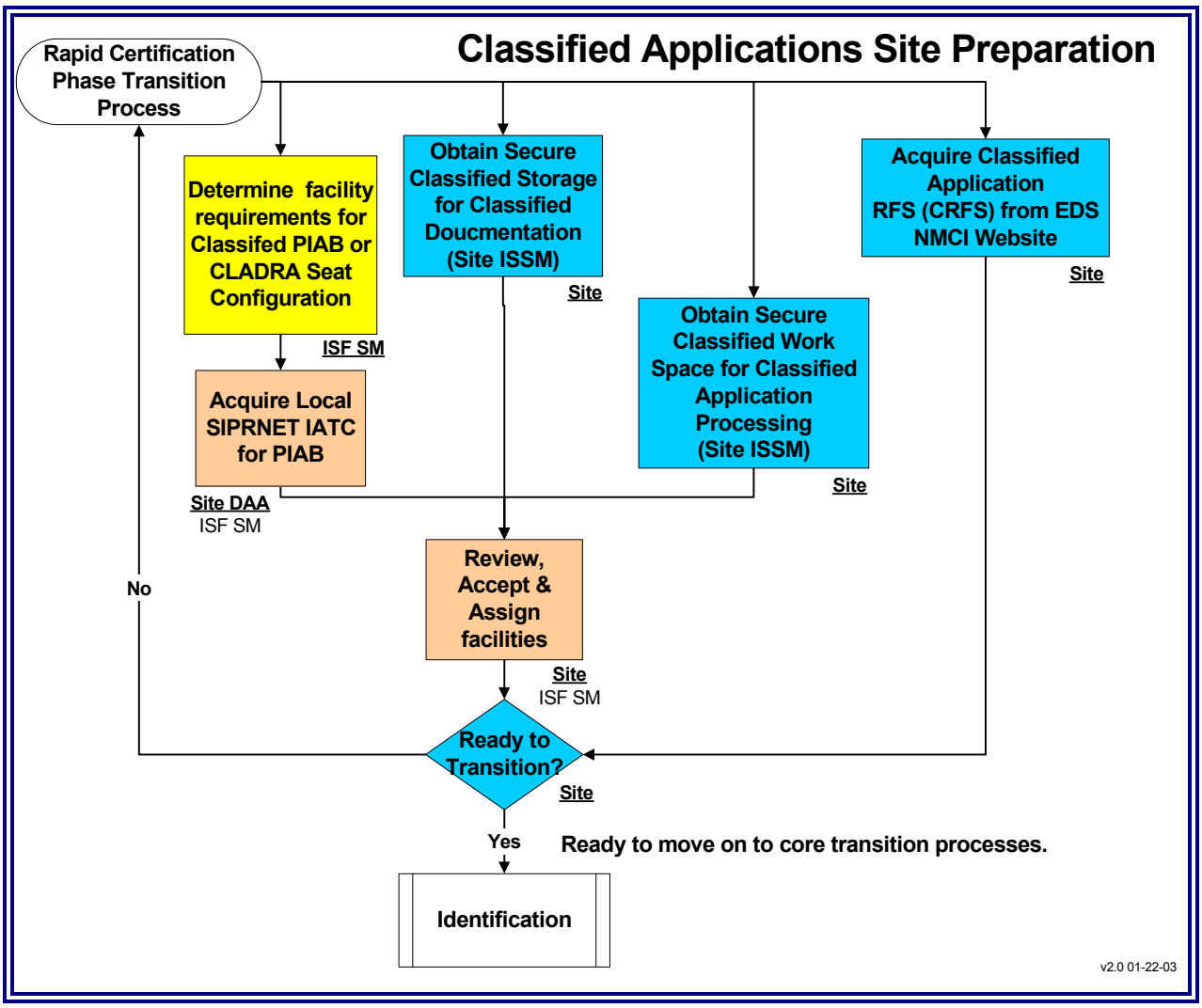


Figure F-3. Classified Applications Site Preparation

Figure F-4 and Figure F-5 depicts the Classified Identification and Rationalization steps.

3.2.1 Classified Application Identification

The Classified Legacy Applications Identification process differs from the unclassified process in the use of the ISF Tools Database. Once the classified applications are identified they are entered into the Classified Legacy Applications Rationalized List template creating the Raw Classified Applications List.

The Classified Legacy Applications Rationalized List format, in Microsoft Excel, can be found on the EDS NMCI website at http://www.nmci-isf.com/transition.htm.

See Figure F-4 for more details of the Classified Legacy Applications Identification process. The remaining steps of the Classified Identification Process are the same as those depicted in the unclassified processes of this guide.

Customers must identify their Legacy Applications on time. Lateness jeopardizes inclusion in Seat Cutover. See Appendix C of this guide for more information on Late Submission.

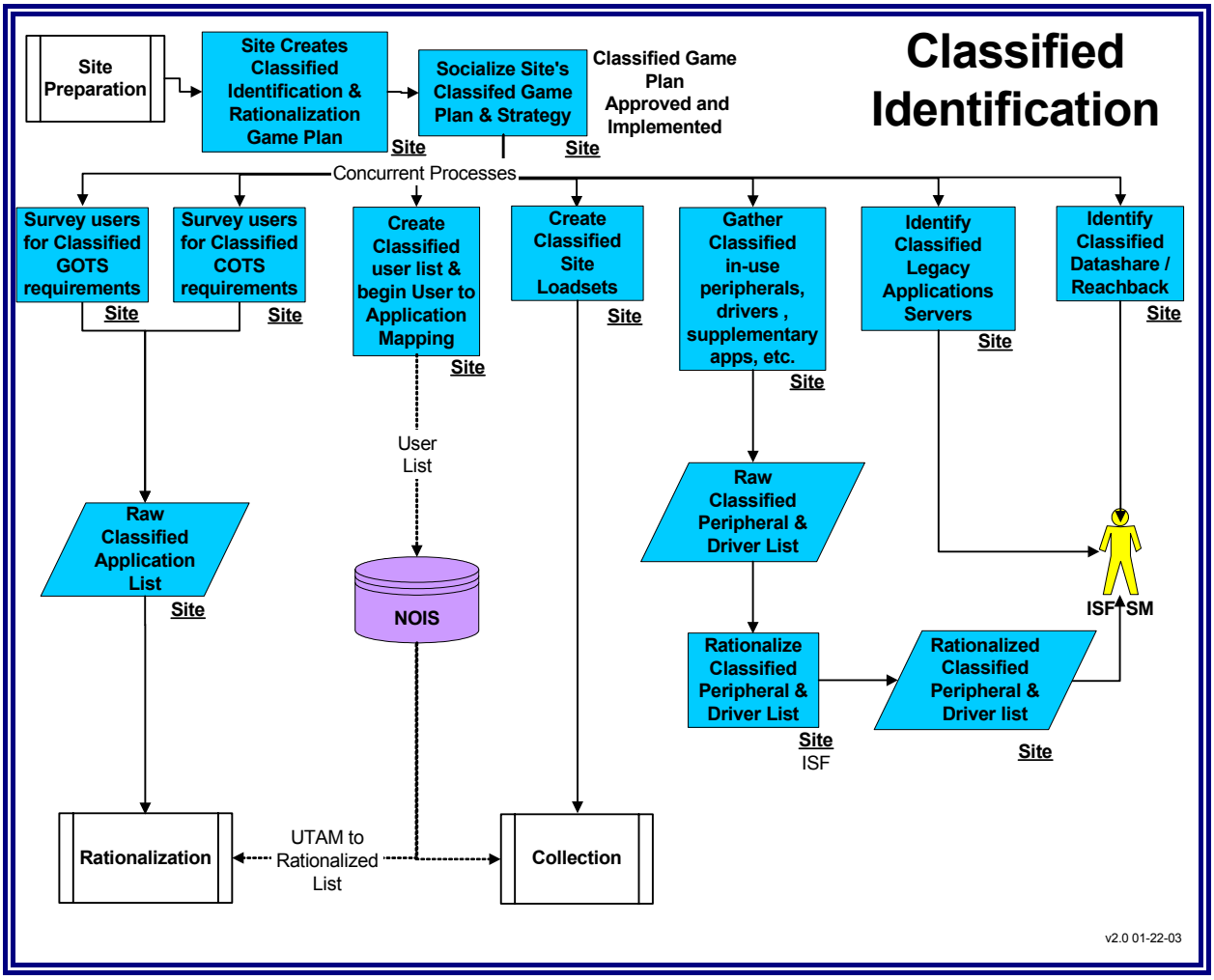


Figure F-4. Classified Identification

3.2.2 Classified Application Rationalization

Once again, the Classified Legacy Applications Rationalization process differs from the unclassified process in the use of the ISF Tools Database. Once the applications have been identified in the Raw Classified Applications List, the Command/Site applies the rationalization steps as depicted in the unclassified processes of this guide. See Figure F-5 for details of the classified application rationalization process.

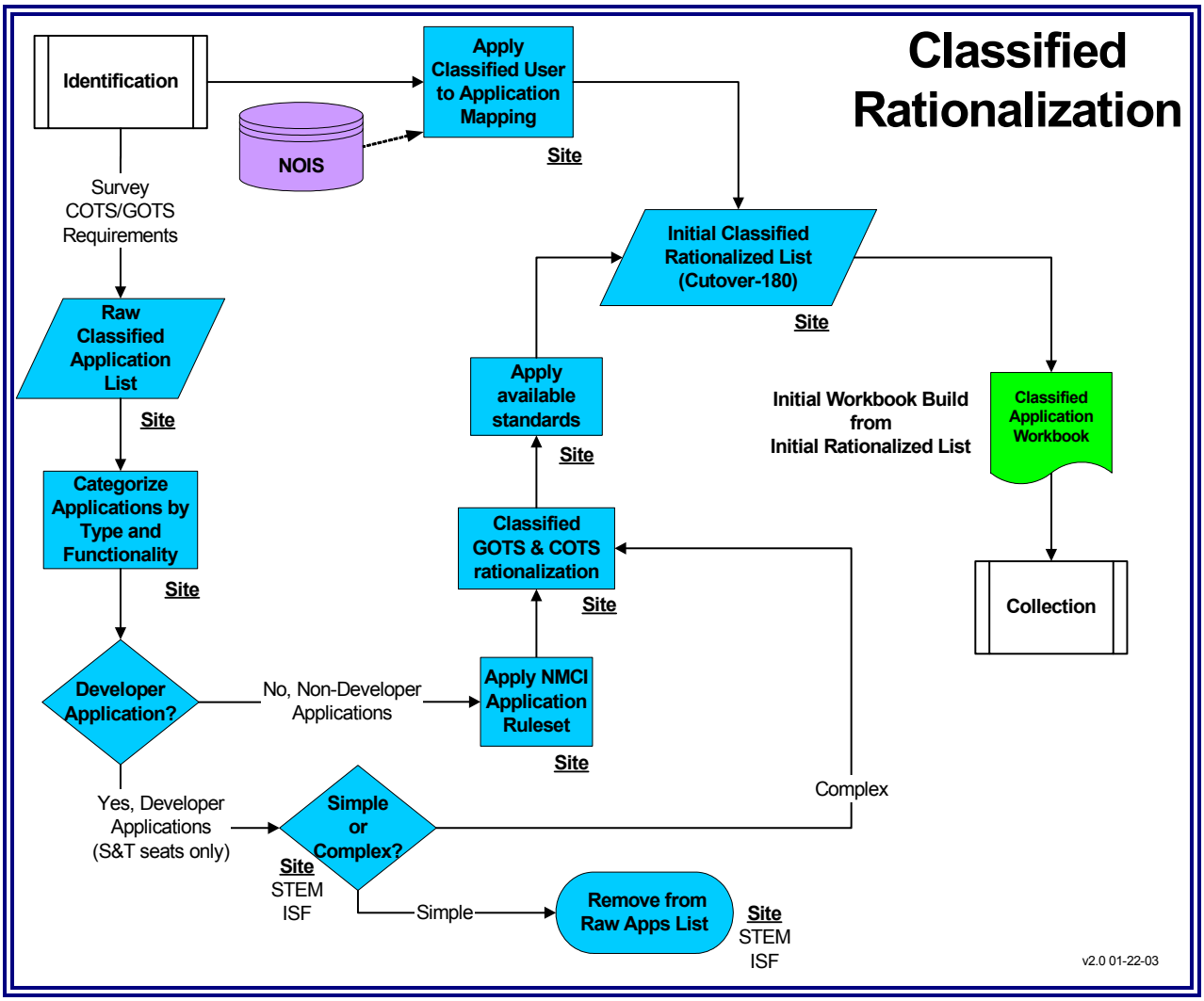


Figure F-5. Classified Rationalization

3.2.2.1 Initial Classified Rationalized List

Those applications from the Raw Classified Applications List that remain after the rationalization process are listed in the Initial Classified Rationalized List.

Instead of using the ISF Tools Database, the site creates the Initial Classified Rationalized List using the template found in Enclosure 2 or downloaded from the EDS NMCI website at http://www.nmci-isf.com/transition.htm.

3.2.2.2 Classified Applications Workbook

3.2.2.2.1 Classified Product Delivery Analyst (CPDA)

There is only one CPDA for all classified applications and he/she is located at the Classified AIT Lab in San Diego, California. The CPDA provides process support on the submission of

classified Legacy Applications, training, Classified Workbook support, data analysis and progress reporting.

In addition, the CPDA will work with on-site SSE Teams to ensure readiness of applications and associated documentation prior to and during testing. The CPDA also works with all members of the Legacy Applications Transition team to ensure proper documentation standards are kept. The CPDA interfaces with government and ISF personnel, including (but not limited to): STEM, PMO, NADTF, DMT, PEO-IT, PDM, SSE Team members, SM, Customer Technical Representative (CTR), LAPOC, AIT, EAGLE and IA Teams. CPDA responsibilities include:

- Review, analyze and provide documentation on LADRA readiness and rationalized list status for the Pre-AOR Review
- Create reports for ISF Legacy Applications management
- Identify applications submitted that already have a documented NMCI solution (Certification by Association (CBA))
- Provide process guidance and Classified Workbook training to ISF and Navy personnel on the submission of Classified Legacy Applications and peripherals
- Investigate media and documentation issues (CRFS, etc.)
- Participate in recurring site status meetings to provide support and problem resolution
- Conduct Readiness Review (RR) and Post Cutover Assessment (PCA) to ensure readiness of site applications and final status

The CPDA will continue to work with a site after Cutover is complete to make sure that the transition is complete and went well.

3.2.2.2 Classified Applications Workbook

The ISF CPDA uses a Microsoft Excel spreadsheet to create the Site Classified Applications Workbook to organize information about the sites' legacy applications as they undergo certification. The Workbooks are created and maintained by the PDA. They initially create workbooks from a customers' Initial Classified Rationalized List of applications. As applications move through the certification and testing processes, the workbook is updated by the CPDA to show status. These updates vary in frequency, but they usually occur weekly and then daily as the site approaches Cutover.

The preferred method for Command/Sites to monitor the progress of their submitted applications is to work the workbook with the CPDA. This interaction usually takes the form of Site-Specific Workbook Reconciliation meetings. These are phone conferences between the CPDA, site LAPOC, the PMO, STEM, and other interested parties. The goal of these conferences is to keep the workbook current so that it portrays a clear picture of a site's applications with respect to

certification. The creation of a workbook usually happens after a Command/Site completes their Initial Classified Rationalized List at Cutover minus 180. The rationalized list and workbooks are considered classified documents, as they may contain classified information.

As applications are entered into the workbook, they are pre-assigned a Classified Request for Service (CRFS) number. This occurs before a CRFS is actually submitted. As the Classified Application Workbook is done manually, CRFS numbers are assigned manually. Then, once the Command/Site submits the CRFS, the pre-assigned CRFS number becomes permanent.

The ISF PDA is responsible for keeping the Command/Site informed on all progress associated with the certification and testing effort. This progress status communication may be accomplished in any number of ways, such as: phone conversations, customer request, designated workbook meetings, etc. The ISF AIT Classified Legacy Applications Lead will utilize the Secret Internet Protocol Router Network (SIPRNET) to pass along more detailed information when required.

3.3 Classified Collection

The Classified Collection process is a Government responsibility. Secure handling procedures, personnel security clearances, custody, and storage are all factors that have to be addressed during this process. Figure F-6 depicts the step of this process.

After the Classified Application Workbook is formulated by the CPDA, the legacy application media and supporting documentation must be collected for submission to the ISF SM for NMCI Certification.

Classified Legacy Applications require the following:

- For Official Use Only (FOUO) CRFS (available at http://www.nmci-isf.com/transition.htm)
- Media and License Verification
- Installation Instructions and Test Scripts
- Network Diagram (desktop-to-server connectivity)
- Test Plan
- Risk Mitigation Engineering Review Questionnaire (RMERQ) (available at http://www.nmci-isf.com/transition.htm - Engineer)
- POC information on Technicians, Programmers or Systems Administrators

Sites do not have to provide proof of all licenses needed for all of the users of an application. However, proof of licensing is required for the copy of the application that is being submitted for NMCI Certification Testing. If a license is not available, proof must be obtained and submitted. Note: In most cases the use of legacy applications without an approved license is a violation of applicable copyright laws and is expressly prohibited. The ISF will test and make recommendations on all legacy application software submitted to them in an effort to facilitate

the efficient movement of seats into the NMCI environment. However, the sole responsibility for ensuring proper maintenance and distribution of licensing for transitioning legacy applications rests with the individual Command/Site/Echelon II/CDA transitioning those applications.

If any prior Interim Authority to Operate (IATO) or DoD Information Technology Security Certification and Accreditation Process (DITSCAP) documentation exists for a legacy application being submitted, it should be collected and stored by the Command/Site for use in the Risk Mitigation Phase. The User-to-Application Mapping (UTAM) must be completed and turned over to the ISF Site Manager. Final UTAM is due with the Final Classified Rationalized List at Cutover -120. Navy Applications Database Task Force (NADTF) will use the UTAM as they perform enterprise rationalization and standardization.

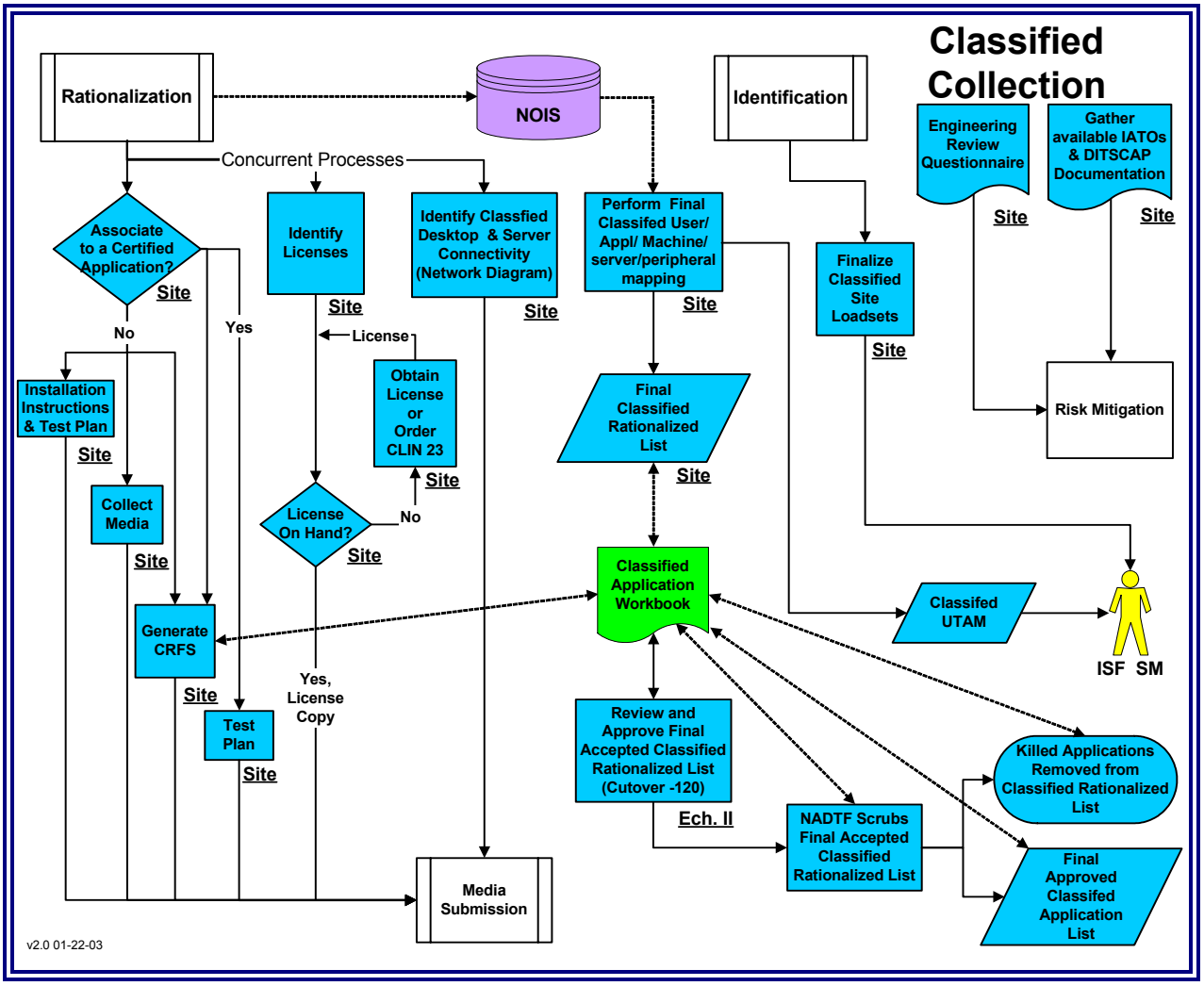


Figure F-6. ClassifiedCollection

3.4 Classified Media Submission

It has been determined that the majority of applications residing on the SIPRNET are Unclassified except when populated with classified data. If the site has an application that itself is classified even without data, the Command/Site will complete the FOUO CRFS form, mark it (classification) appropriately, prepare the media, and submit both to the ISF SM.

Classified Legacy Applications Media Submission *(*Figure F-7*)* is different from the Unclassified Media Submission in the adherence to appropriate security procedures for handling and storage of classified information. The Command/Site Information System Security Manager/Officer (ISSM/O) will be responsible for securing all classified software and documents. The Command/Site ISSM/O will review all completed RMERQs and Network Diagrams provided to the ISF SM and/or the ISF Site Solutions Engineering (SSE) Team Lead to determine their classification due to the level of detail they contain.

If they become classified material, the appropriate handling procedures are invoked per the level of classification. RMERQs and Network Diagrams are required for on-site or off-site testing and certifications. All applications will require the RMERQ form completed prior to the Risk Mitigation Phase. The ISF will not have secure storage facilities on-site; the Site ISSM/O is required to provide secure storage and ISF access.

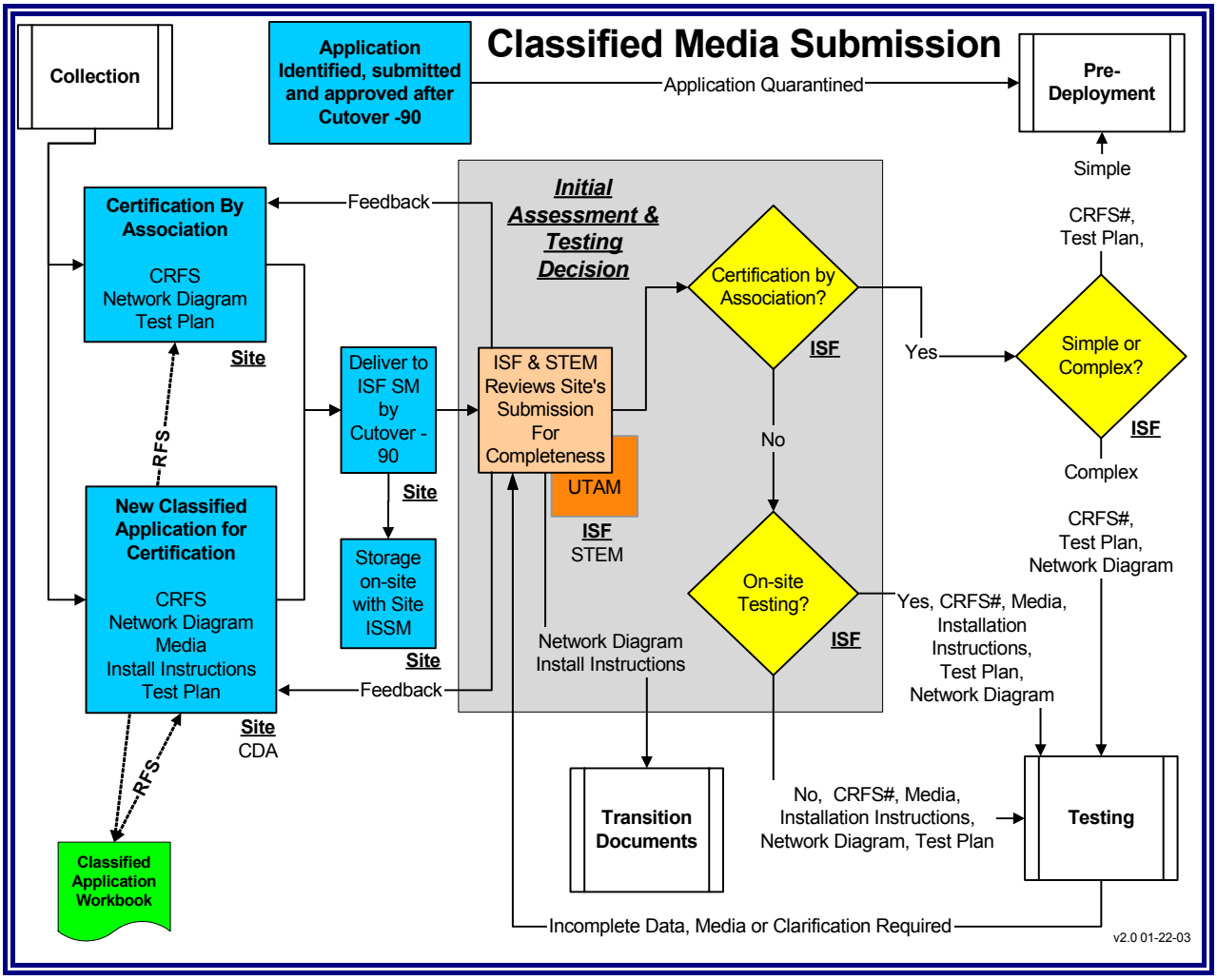


Figure F-7. Classified Media Submission

After an application's media and support materials are collected, they must be submitted to the on-site ISF SM to begin the NMCI Certification process. If the ISF SM has not arrived on site, the Command will hold all materials until the ISF SM arrives. Tracking at the ISF level will commence upon receipt of the material. Each application will be assigned a tracking number ('CRFS Number') by the PDA.

The ISF SM will turn the submission over to the ISF SSE Team Lead. The ISF and STEM teams will perform an initial assessment of the submission in the Completeness Review. If any parts of the required submission are missing or incomplete, the STEM and ISF will work with the Command/Site to provide them. If the submission passes the completeness review, the ISF then determines which testing activity the application will be sent to for processing.

In most cases the scheduling of applications for certification/testing will be done by the on-site SSE Team. Further, the SSE Team Lead will determine whether Testing will occur on-site via the CPIAB and/or the Classified NMCI Test Seat in the Local Deployment Solutions

Development and Testing (LDSD&T), or sent for Certification to the Classified Application Integration & Testing (AIT) Lab located at the San Diego Network Operations Center (NOC).

Submission Deadlines

All applications are due to the ISF SM NLT Cutover minus 90.
Any applications submitted late are subject to the Late Identification and Submission Process. (See Appendix E.)

3.5 Testing

The Government and the ISF share joint responsibility in this process, but the ISF conducts most of the work.

Testing is broken down into two separate areas, each performing a unique and specific function necessary in the preparation of a transitioning application and comprising the core transition methodologies capable of covering a wide range of software and application implementation strategies. These two separate areas are the Lab Testing and On-Site Testing.

Once the completeness review is done, the ISF SM and STEM make a determination on the best method to process an application for inclusion in NMCI. Four testing approaches are available:

- Classified San Diego Packaging and Certification Lab (CAIT)
- PIAN
- PIAB
- LDSD&T

The PIAB and LDSD&T are done on site and the other two (PIAN and the Classified San Diego Packaging and Certification Lab) are accomplished off site. For all practical purposes the methods used in the processing of classified applications are identical to those used in the unclassified process, the only differences being the manual tracking through the Classified Workbook and the special security requirements for storage, handling and personnel clearances.

In the Testing processes there are two distinct methods available for preparing an application for inclusion on an NMCI seat: Local Deployment which is done at the site and involves preparing the application for manual distribution to the desktop (Local Deployment) and centralized distribution (Push via Novadigm Radia) which is accomplished at the Classified San Diego AIT Lab or the PIAN. There are no significant differences in processing classified legacy applications via Local Deployment or Push, except where previously described in this appendix.

During the testing processes the application status is recorded and tracked in the Classified Workbook. The Classified PDA, AIT Lab personnel and SSE teams will record the status of the various steps in the process.

3.5.1 Local Deployment vs. Push

As indicated in the main guide the application will be Pushed or Local Deployed to the desktop. The methods, steps, procedures, and processes for deploying applications in the classified environment are the same as in the unclassified environment, with the exception of the special security considerations for classified applications.

NOTE: The ISF has the responsibility to determine the most effective way to deploy a Legacy Application, and they will route the Legacy Application to the appropriate testing location and method.

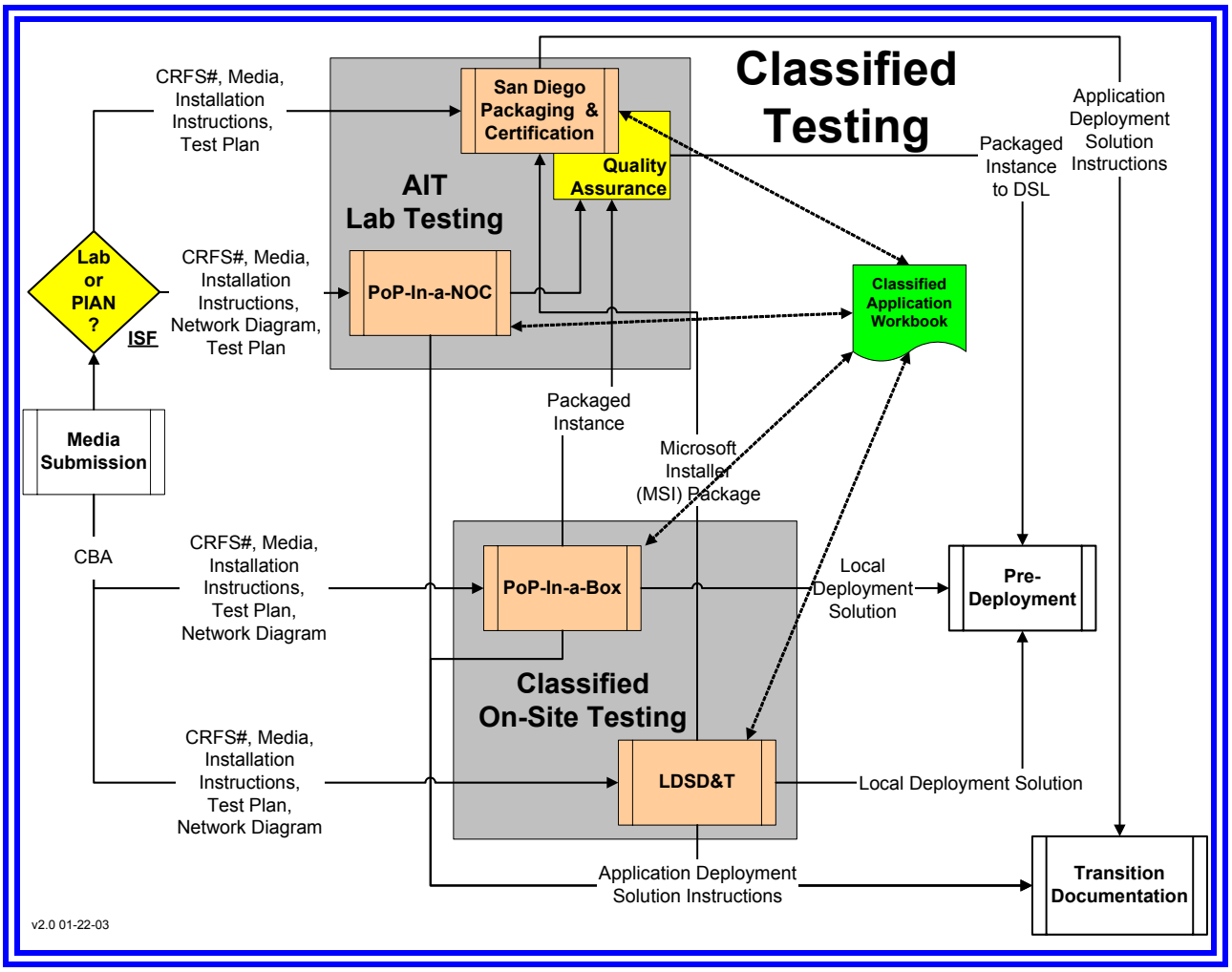


Figure F-8. Classified Media Submission

3.5.2 San Diego Classified Packaging & Certification

Those applications selected for San Diego Packaging and Certification are sent to the San Diego Classified Application Integration and Testing (CAIT) Lab by the ISF with the help of the ISSM/O. Figure 8 depicts the Classified Packaging and Certification Lab processes. Applications go though a Packaging Audit by ISF personnel in the lab to verify that the packet is complete and that the media submitted is valid with no viruses. Any installation instructions are tested for completeness. The site is notified of problems with any submissions via SIPRNET by the ISF AIT Classified Legacy Applications Lead. With the exception of manual tracking through the Classified Workbook and the NMCI Certification Letters, which will be generated soft-copy and transmitted via E-mail or SIPRNET, all of the procedures in this process are the same as those depicted in Section 4.0 of the main guide.

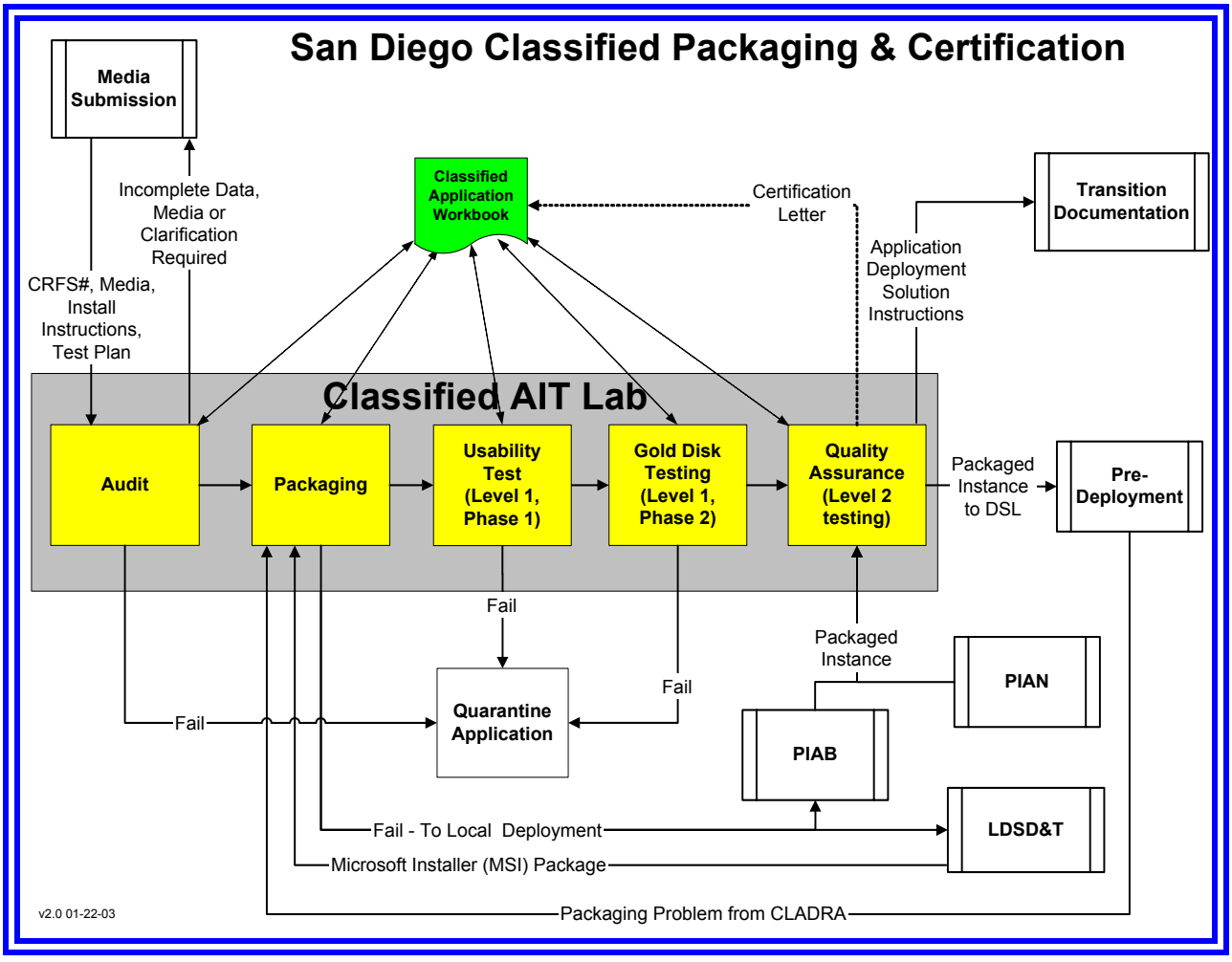


Figure F-9. San Diego Classified Packaging and Certification

3.5.3 PoP-In-A-NOC (PIAN)

Figure F-10 depicts the PIAN process. The PIAN is mostly used by the ISF to process CDA applications and provide enterprise solutions. However, the ISF may use the PIAN to provide solutions for transitioning Classified Legacy Applications. The PIAN operates in a secure environment within the Network Operations Center (NOC). Therefore both classified and unclassified media may be processed through the same equipment. With the exception of manual tracking through the Classified Workbook, SIPRNET, and special handling requirements, all of the procedures in this process are the same as those depicted in section 4.0 of the main guide.

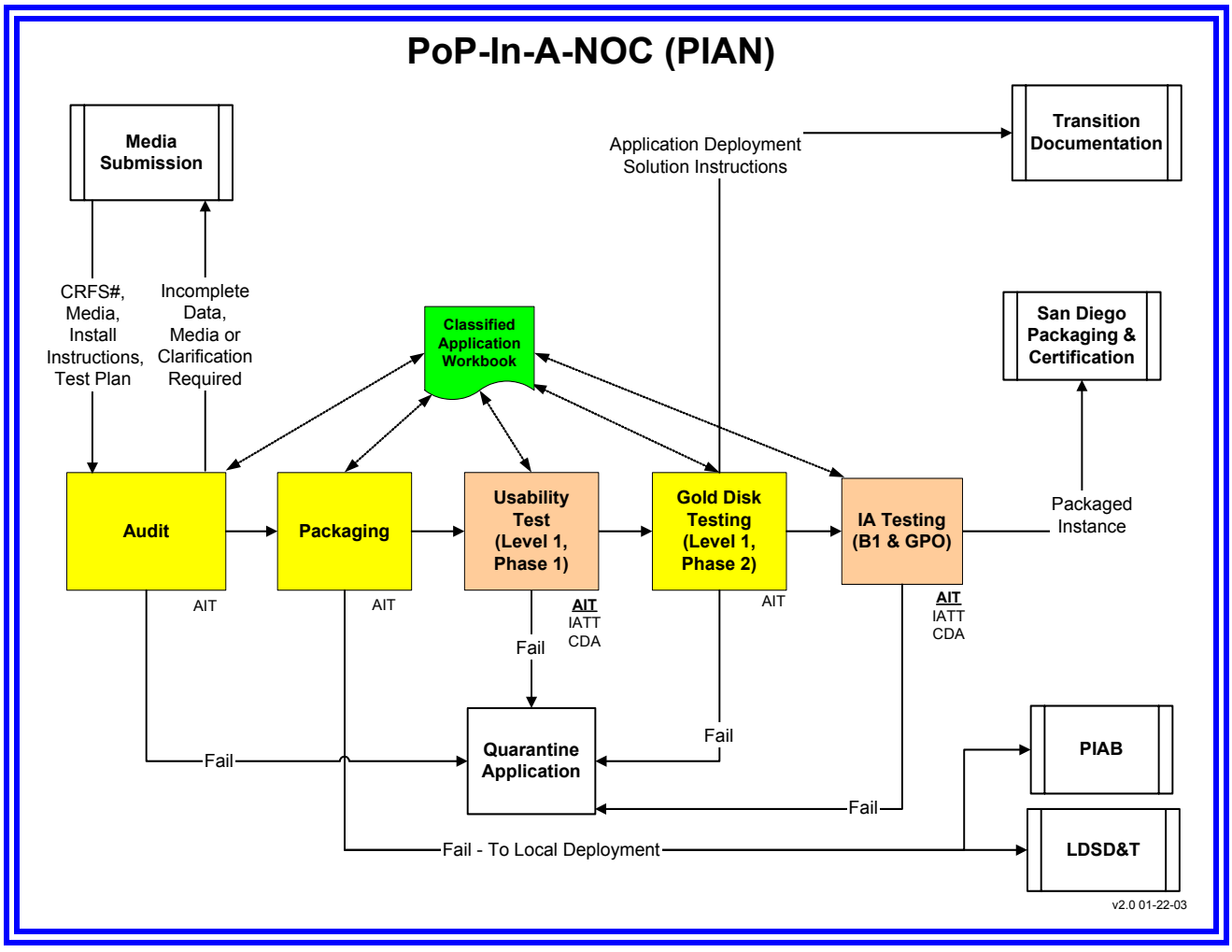


Figure F-10. PoP-In-A-NOC

3.5.4 On-Site Testing

Applications retained on-site for Local Testing are evaluated for their suitability for packaging and electronic push to the desktop. Applications selected for local packaging will proceed through Packaging steps by the ISF Site Solutions Engineering (SSE) team using the CPIAB, if

available. Those selected for Local Deployment will be processed through the CPIAB or run through LDSD&T. There are no significant differences in processing classified legacy applications with regards to On-Site Testing, except where previously described in this appendix.

3.5.5 Classified PoP-In-A-Box (CPIAB)

The CPIAB is a separate suite of equipment from the unclassified PIAB. Classified applications may not be processed on an unclassified PIAB. Because there are so few CPIABs, a Command/Site may not receive the use of this tool and may have their applications processed through the Classified AIT Lab or PIAN.

Processing classified applications through the CPIAB does not differ significantly from the unclassified processes, with the exception of the manual tracking of the Classified Workbook and the special security requirements for storage, handling and personnel clearances.

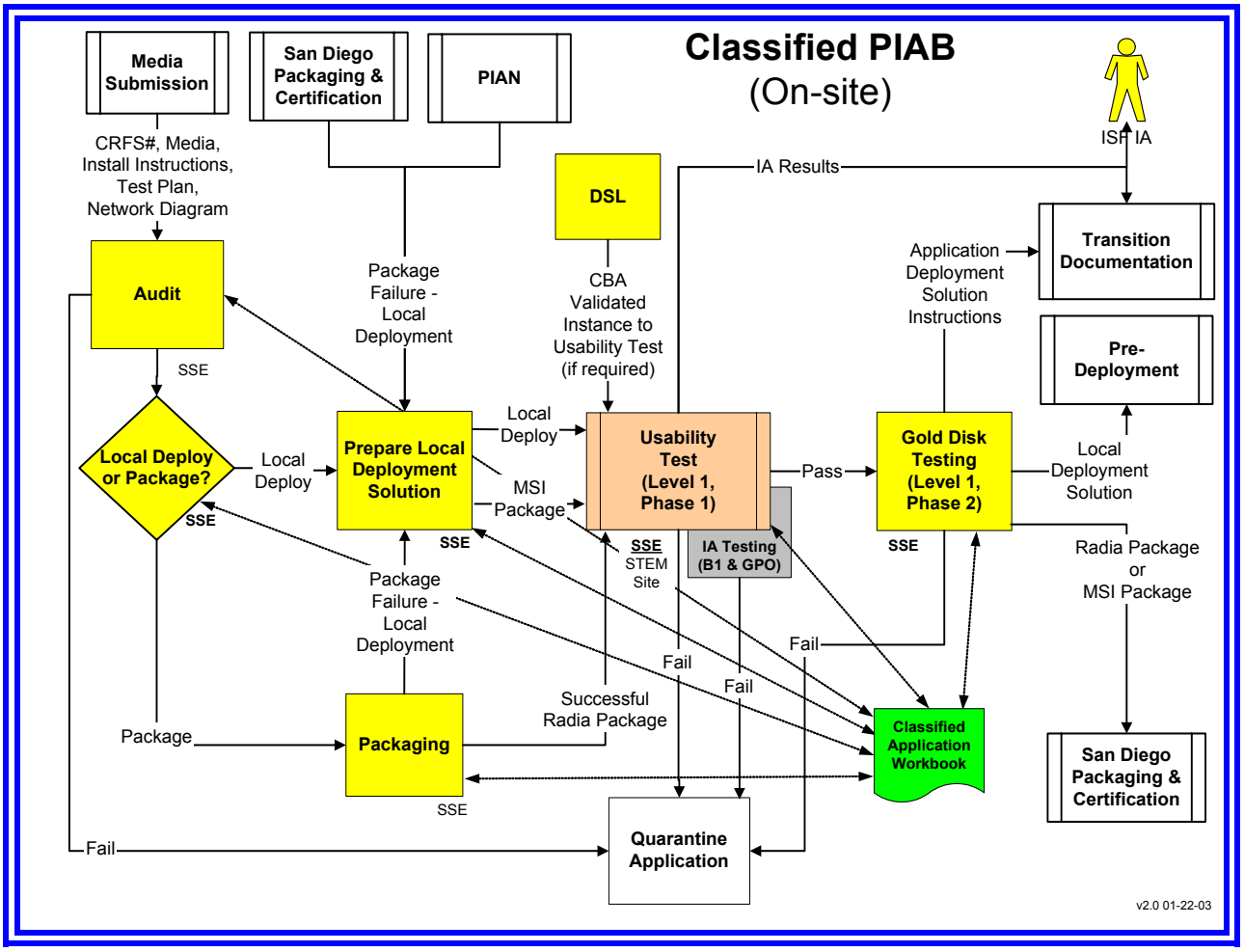


Figure F-11. Classified PoP-In-A-Box

3.5.6 Classified Local Deployment Solutions Development and Testing (CLDSD&T)

When a CPIAB is not available or deployed on-site, the SSE team will use an NMCI Test Seat to develop local deployment solutions for applications when the NMCI infrastructure is installed and active.

The Classified NMCI Test Seat will be used in the same manner as in the processing of unclassified applications, in the Rapid Certification Phase, to perform the Classified Usability Test. As indicated in Classified Site Preparation, where the requirements for processing of classified legacy applications were identified, application testing will be done on a Classified NMCI Test Seat that is housed in a secure environment.

The steps in the CLDSD&T do not differ significantly from those of the unclassified LDSD&T. The main differences are the use of the manual tracking of the Classified Workbook and the special security requirements for storage, handling and personnel clearances. The CLDSD&T process is depicted in Figure 12. During the CLDSD&T process, the testing and certification status is recorded and tracked in the Classified Workbook by the SSE team and the Classified PDA.

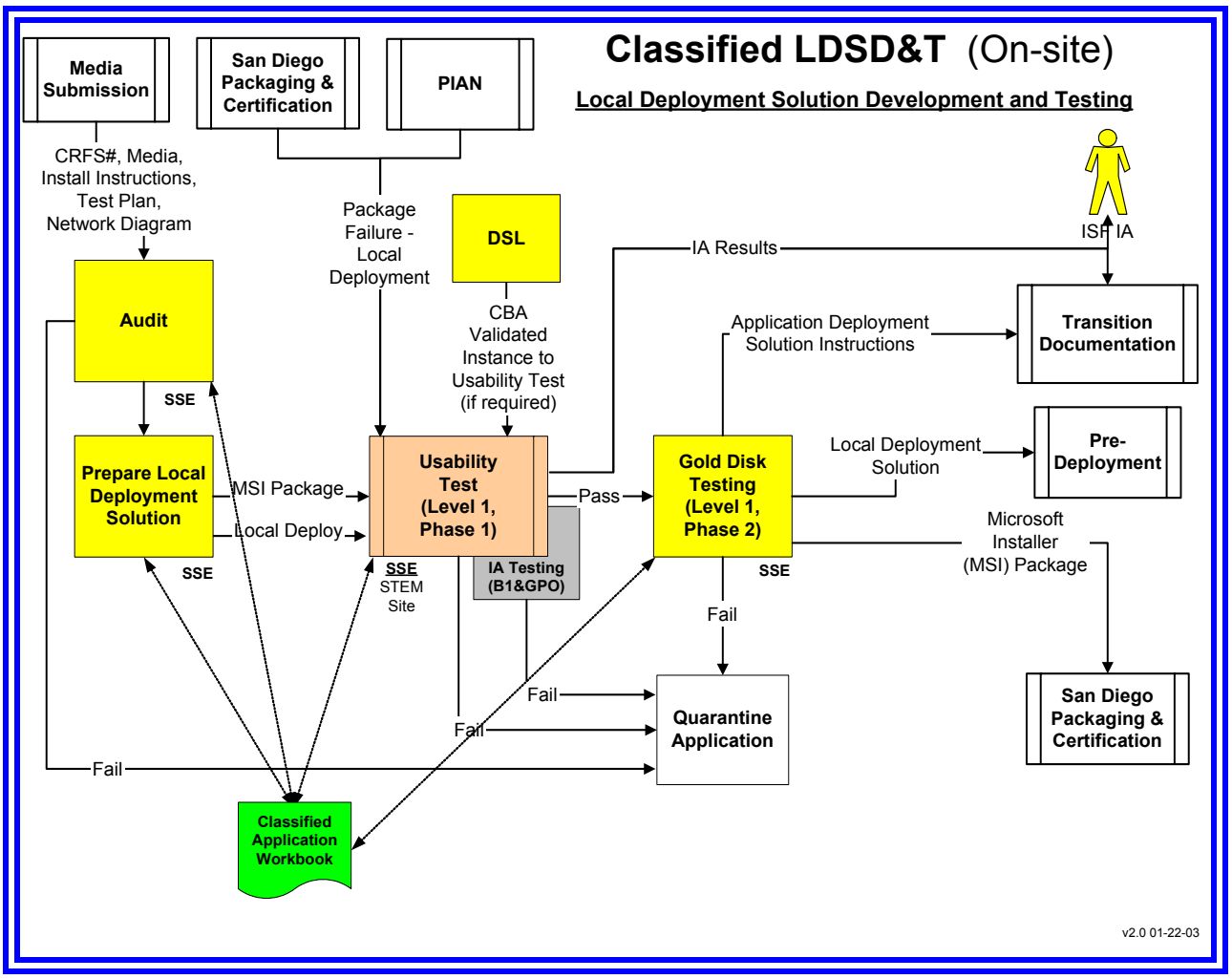


Figure F-12. Classified LDSD&T

3.6 Classified Application Transition Documentation

The Transition Documentation process is an ISF responsibility. The process is the same for classified and unclassified applications, with the obvious exception of the storage of the documents.

3.7 Information Assurance

The Classified NMCI Information Assurance (IA) process is similar to the Unclassified IA process except that there are no Boundary 2 (B2) and Boundary 3 (B3) requirements. Only Enterprise Boundary 1 (B1) and Boundary 4 (B4 or Group Policy Object (GPO)) are utilized in the Classified NMCI architecture. The Risk Mitigation Phase remains the same for classified and unclassified legacy applications and is beyond the scope of this guide. All other components, policies and procedures remain the same as the Unclassified NMCI environment depicted in the Guide.

3.8 Classified Pre-Deployment

The Pre-Deployment process is primarily an ISF responsibility. The Classified Pre-Deployment Process is the same as the Unclassified Pre-Deployment process, except the Classified Workbook replaces the ISF Tools Database and the Certification Letters are generated manually. In this stage, the final preparations are made before actual delivery of user seats. Figure F-13 shows the Classified Pre-Deployment process.

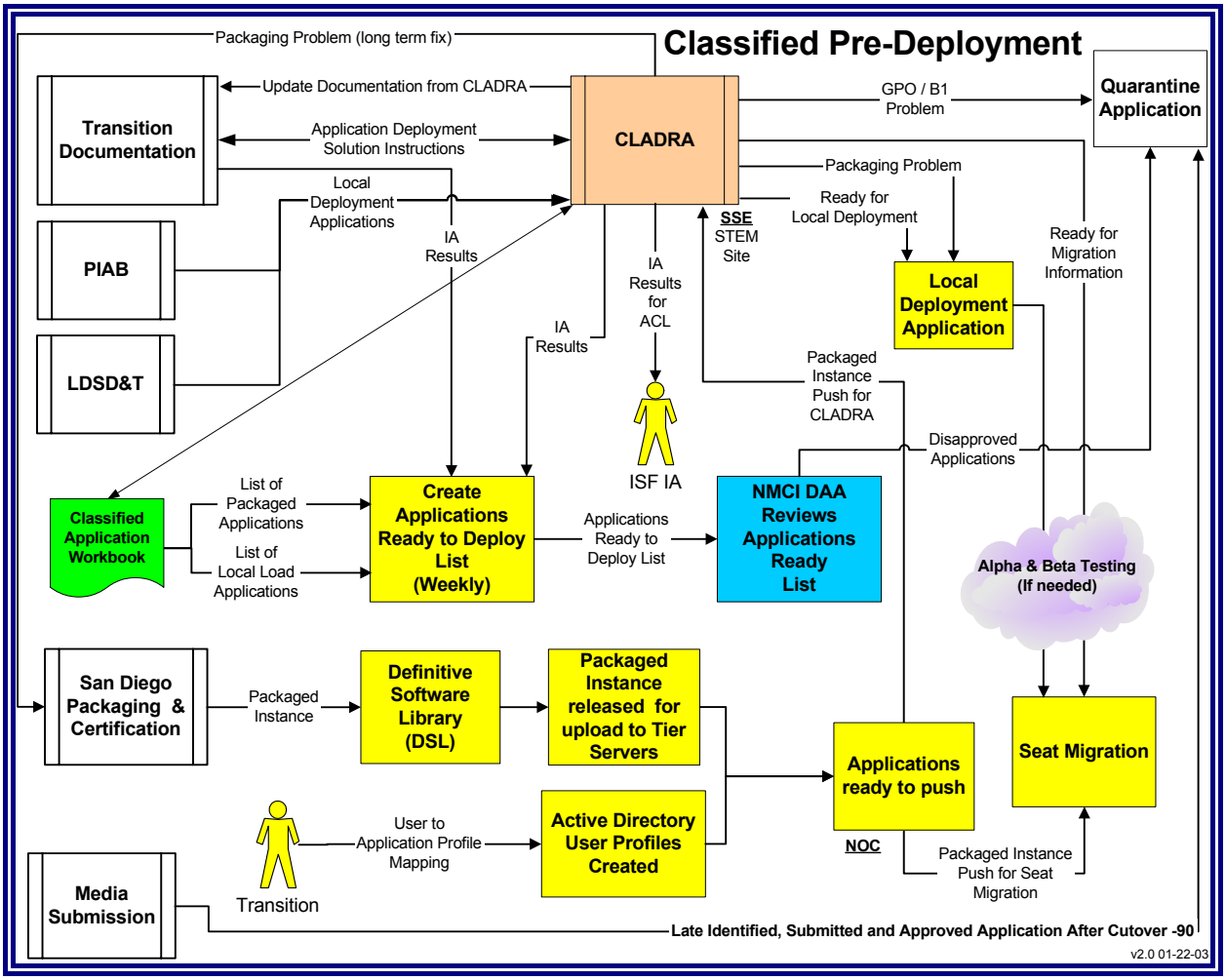


Figure F-13. Classified Pre-Deployment

3.8.1 Classified Legacy Application Deployment Readiness Activity (CLADRA)

The Pre-Deployment test is CLADRA. The CLADRA testing is a joint sub-process that is primarily an ISF responsibility.

CLADRA testing is conducted by the ISF in the live NMCI environment. The goal of CLADRA is to test 100% of the applications to be deployed to NMCI. In some instances, testing all

applications may not be practical. The CLADRA test is designed to verify the transition solutions for the legacy applications. The steps of the CLADRA process do not differ significantly from the unclassified LADRA process. The use of the Classified Workbook to track status is the main difference.

All applications that successfully complete CLADRA testing are ready for Local Deploy or NOC Push to Seat Migration (Cutover).

Upon successful completion of CLADRA, the legacy applications are ready for the initial seat migration (Cutover).

Quarantine

Typically a Quarantined application is one that is prohibited from operating in the NMCI environment due to failure in one or more areas of the NMCI Ruleset or testing. Applications that are Quarantined are left to operate in the Legacy environment. Failures can occur for many reasons, such as: inability to operate in Win 2K, different operating system, interfere with the Gold Disk, violate GPO/B1/policies, identified/submitted too late to process, no user/tester support, and/or network connectivity errors. Some applications that violate the NMCI Ruleset will be Killed and removed from the Rationalized List. These Killed applications will not be utilized in NMCI and **will not** be Quarantined.

The guidelines for Quarantined applications do not differ from the unclassified process.

4.0 —CONCLUSION

The transition of classified legacy applications is not significantly different from the processing of unclassified legacy applications. With the exception of special handling, security, and storage procedures, manual tracking via the Classified Workbook, most of the steps, procedures and processes remain the same as the unclassified processes depicted in the main portions of this guide.

For Official Use Only (FOUO)
Classified Request for Service (CRFS)

(When Filled In) CRFS #

Site: Please fill out all fields in the Site section then submit this form to NMCI.
Important: Please fill out all fields. If no information is needed, put N/A.

FILLED OUT BY SITE

1.	Site Name:		
2.	UIC:	Command Name (PLA):	
3.	Address Line 1:		Address Line 2:
4.	City, State, Zip:		Country:

Site Transition Manager

5.	First Name:		Last Name:
6.	Phone:	E-mail:	

Legacy Applications POC

7.	First Name:		Last Name:
8.	Phone:	E-mail:	

Application On Site SME

9.	First Name:		Last Name:
10.	Phone:	E-mail:	

Application Information

11.	COTS / GOTS? (Select One)	
12.	Application Full Name:	Application Acronym:
13.	Application Version:	
14.	Web Application: Yes/No (Select One)	If yes, URL:
15.	Software Dependencies:	
16.	Hardware Dependencies:	

Application Vendor (COTS)

17.	Company Name:	
18.	Company Phone:	Company Website:

Central Design Authority (GOTS)

19.	POC First Name:		POC Last Name:
20.	POC Phone:		POC E-mail:
21.	UIC:	Command Name (PLA):	

(Continued next page)

FILLED OUT BY SITE (CONT.)

Installation Information

Document ID	Version	Effective Date	Document Owner	Stored	Min Retention	Disposition
700-W02FB	1.08	2002/06/30	Kerry Powell	Web Page	N/A	N/A

Enclosure (1)

For Official Use Only (FOUO)

Classified Request for Service (CRFS)

(When Filled In) CRFS #

22.	Installation Configuration: Client / Server / Both (Select One)
23.	Type of Installation: Full / Minimum / Custom (Select One) Description:
24.	Application License Type: License / Shareware / Freeware / Unknown (Select One)
25.	License Serial Number (if needed):
26.	Installation Key:
27.	Required Patches / Updates / Service Packs:
28.	Installation Instructions: (If more room is needed, provide on file on media)

Current Configuration Information

29.	Server Drive Mapping:
30.	Test Scripts Required: Yes/No (Select One) If Yes, provide name of files on Media:
31.	Test Data Required: Yes/No (Select One) If Yes, provide name of files on Media:
32.	Special Access / User Privileges / Logon/Password information:
33.	Additional / Special Instructions:

Shipping Information

34.	Shipping Carrier: UPS / FedEx / Airborne / DHL / US Post Office / Hand Delivered (Select One) If Other:
35.	Mode of Transportation: Air / Ground (Select One)
36.	Carrier Tracking / Shipping Number:
37.	Date Shipped: (ccyy-mm-dd)

FILLED OUT BY LAB SCHEDULER

38.	Is this RFS form sufficiently complete and accurate? Yes / No (Select One) If 'No', describe:
39.	Review Date (dd-Month-ccyy): Time (h:mm am/pm):

Enclosure (1)

Classified Legacy Application Rationalized List Template

	Command/Site Name:	UIC Number:	Plain Language Address:	UIC Primary POC Name:	UIC Primary POC E-mail:	UIC Primary POC Phone Number:					
RFS or Referencing RFS	**Full Application Name**	**Acronym**	**Operating System**	**Major Version Number**	**C=COTS G=GOTS**	**Functional Area**	**Number of Licenses**	**Stand-Alone / Server Based**	**Mission Criticality**	**Status**	**Comments**

Appendix G — Templates, Samples, and Examples

G.1 Site Representation of Legacy Peripherals Template

Legacy Desktop Peripherals Requested for NMCI Transition								
Site Name:		Cutover Date:						
List Prepared By:		Preparation Date:						
Preparer's E-mail Address:		Preparer's Phone #:						
Manufacturer	Device Type	Device Name/ Model	If there is any bundled application associated with this device that has been added to your site's Legacy Application Rationalized List, list the application's RFS # and name here.	If there is a driver required that is not the default Windows 2000 driver, list it here.	User Name	Domain	Net ID	Comments
Example:								
Epson	*Printer*	*Stylus Color 850N*	*#123 Printer Pal*		*John Doe*	*CMDHQ*	*JDOE*	

Site Name: This is the official name of this site as it appears in the ISF Tools.

Cutover Date: This is the official scheduled Cutover date for this site.

List Prepared By: This is the name of the person designated by the site to create this list.

Preparation Date: This is the date that this list was created.

Preparer's E-mail Address: This is the email address of the person designated by the site to create the list.

Preparer's Phone #: This is the phone number of the person designated by the site to create the list.

Device Type: Examples: Printers, scanners, monitors

Device Name/Model: Enter the exact name and model number of the device.

If there is any bundle application associated with this device that has been added to your sire's Legacy Application Rationalized List, list the application's RFS# and name here. An example would be photo-editing software that was bundled with a scanner. By doing this RFS is created. If you don't know the RFS number, it can be found in the site's Legacy Application Rationalized List in the ISF Tools Database.

If there is a driver required that is not the default Windows 2000 driver, list it here. By default, the ISF will attempt to the Windows 2000 driver for this peripheral. However, many devices have drivers that provide additional functionality than the default driver. List the file name of the driver here. The site will be required to provide this driver to the ISF if testing is required. There maybe a CLIN 29service fee for any additional testing and reengineering. If the driver is not Windows 2000 compatible, impacts SLA performance or violates NMCI security policies it will not be allowed.

User Name: This is the user whose NMCI seat will connect to the device.

Domain: This is the user's new NMCI Domain.

Net ID: This is the user's new NMCI Net ID.

G.2 Example Installation Instruction

The following is an example of an installation instruction that the ISF will use to install the release for testing.

Visio2000: Revised Network Installation Instructions (Network.wri) for
Visio 2000 Standard Edition
The information in this article applies to:
Microsoft Visio 2000 Standard Edition
This article was previously published under Q258467

SUMMARY

The Network.wri file that is included with Microsoft Visio 2000 Standard Edition contains incorrect instructions for how to perform a network installation.

This article contains the full text of the Network.wri file, with the corrections incorporated. Use the information in this article instead of the Network.wri file when you need to do either of the following:
Install Visio 2000 Standard Edition to a network drive for shared use.
-or-
Install Visio 2000 Standard Edition locally from a network drive.

MORE INFORMATION

Visio® 2000 Standard Edition
Network Installation Instructions

File version 6.0.0 Visio(R) 2000 Standard Edition US English version
Network Installation Instructions
This file contains information about setting up and running Visio 2000 on a network.
We recommend that you read this file and keep a printed copy with your Visio documentation.
For other late-breaking information about installing and running
Visio 2000, see the README.WRI file. For a list of all the files copied to your hard drive if you install the complete version of Visio 2000, see the
FILELIST.WRI file.

CONTENTS

1. NETWORK LICENSING INFORMATION

To run Visio on a network that gives more than one-person access to the product, you need to acquire additional licenses either by purchasing additional retail packages of Visio or by purchasing license packs.
A license pack, which authorizes one additional user, includes a product license, a serialized registration card, and a documentation order form.

2. OPERATING SYSTEM REQUIREMENTS FOR VISIO 2000

To use Visio 2000 Standard Edition, you must be running one of the following 32-bit Microsoft Windows operating systems:

- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows NT 4.0 (Service Pack 3 or later is required)

Service Packs for Windows 95, Windows 98, and Windows NT operating systems can be obtained from Microsoft Corporation (www.microsoft.com).
NOTE: To install Visio 2000 on a workstation running Windows NT 4.0, the user installing the product must have Administrator privileges for that workstation.
NOTE: Installation Path Length Limitation: To ensure operation of the Visio 2000 Solutions the directory chosen for installation of Visio 2000 Standard Edition must have a path name of less than 55 characters in length.

3. NETWORK SETUP OVERVIEW

Setting up Visio on a network is a two-step process: First, you install Visio on the network server; second, you set up individual workstations so they can run Visio from the server or from each workstation's hard disk.
NOTE: Setting up Visio 2000 on a network server for shared use requires Windows NT 4.0 SP 3 or later. This procedure is not supported under Windows 95 or Windows 98.
For details about setting up Visio on a network so that multiple workstations can use a shared copy from the server, see "SETTING UP VISIO 2000 ON A NETWORK SERVER FOR SHARED USE" below.
For details about setting up Visio files on a network server so that the program can be loaded onto the hard disks of individual workstations, see "SETTING UP VISIO 2000 ON A NETWORK SERVER FOR LOCAL INSTALLATION TO WORKSTATIONS" below.

4. PREPARING A WORKSTATION TO SET UP VISIO FOR SHARED USE

The Visio 2000 setup program is based on the Microsoft Installer (MSI) technology. MSI must be installed on the workstation you are using to set up Visio 2000 for shared use before starting the Visio 2000 setup program. If MSI is not installed on the workstation, or if you are in doubt, use the following procedure to install MSI:

1. Insert the Visio 2000 CD into your CD-ROM drive.
2. From the Start menu, choose Run.
3. Type d:\Install\bin\sp\MSI\WinNT\InstMSI, where d is the letter assigned to your CD-ROM drive.

After installing MSI, complete the following procedure to install Visio 2000.

5. SETTING UP VISIO 2000 ON A NETWORK SERVER FOR SHARED USE

To install Visio 2000 on a network server for shared use:

You must have write access to the network server to install Visio on the server.
NOTE: Do not run the Setup.exe file located in the root directory of the Visio CD for this procedure. This file is for single-user installations only, and will not install Visio correctly for shared use.
1. From a workstation running Windows NT 4.0, log on to the network and connect to the drive where you want to install the Visio program.
2. Insert the Visio 2000 CD into your CD-ROM drive.
3. From the Start menu, choose Run.
4. Type d:\Install\Setup /a where d is the letter assigned to your CD-ROM drive.
Setup prompts you for the location of your Visio installation.
5. Type e:\visio, where e is the letter assigned to the network server and Visio is the directory on the server where the Visio program files will reside.
6. Follow the instructions on your screen.
Setup /a installs the Visio program files and creates the following subdirectory: Visio\Bin, for Visio product files.
To set up a workstation to run Visio from a network server:
1. On the workstation, from the Start menu, choose Run.
2. Type e:\Visio\setup, where e is the drive letter and \Visio is the directory on the server where the Visio setup program resides.
3. Follow the instructions on the screen.
The workstation setup does the following:

- Installs or updates any Windows system and shared files required by Visio.
- Adds Visio 2000 to the Start Menu.

6. SETTING UP VISIO 2000 ON A NETWORK SERVER FOR LOCAL INSTALLATION TO WORKSTATIONS

You can place Visio 2000 files on a network server by following the steps in the preceding section, "SETTING UP VISIO 2000 ON A NETWORK SERVER FOR SHARED USE." Then, users can connect to the directory and run the Setup program to install Visio on their workstations.
To install Visio 2000 from a network server to a workstation
1. On the workstation, from the Start menu, choose Run.
2. Type f:\visio\setup where f is the drive letter and Visio is the directory on the server where the Visio setup program resides.
3. Follow the instructions on the screen.
4. When Setup prompts you for an installation location, type c:\program files\Visio, where c is the letter assigned to the workstation hard drive and \program files\Visio is the directory on your workstation where the Visio program will reside.

7. DEFINING DEFAULT FILE PATHS FOR VISIO FILES

Users can define default file paths for Visio drawings, templates, add-ons, and filters. To specify these custom paths, choose Options... from the Visio Tools menu, and then click the File Paths tab. File paths defined here are written into the user's registry under the HKEY_LOCAL_MACHINE\Software\Visio\Visio 2000 key. Click the Help button on the File Paths tab for more information.

8. OPENING VISIO FILES ON A NETWORK

Working with and opening Visio files on a network is essentially the same as on an individual workstation. On the network, however, you can make a drawing available to other users and allow them to make changes to the file. You can also protect the file from changes.

* Keep the following issues in mind when using Visio on a network:

You can share stencil files so that multiple users can access them at once. However, when you share stencil files, it is important that users not open them in read/write mode. (When a Visio drawing file is opened in read/write mode, no other network user can access the file.)

By default, the read-only attribute is set for stencil files to prevent users from opening them in read/write mode. You can also set the network Visio directory to read-only to prevent users from opening the files in read/write mode.

9. USING FILTERS WITH VISIO IN SHARED WINDOWS ENVIRONMENTS

If you are using Visio 2000 in a shared Windows environment in which system files are write-protected, Visio 2000 cannot store custom filter settings. You will need to make changes to any filter defaults each time you use that filter – changes will not be retained from one use to the next.

Visio 2000 Standard Edition

END of Network Installation Instructions

G.3 Example for Installation Instruction: Defense Information Infrastructure/Common Operating Environment

Defense Information Infrastructure (DII)

Common Operating Environment (COE)

Installation Procedures (IP) for <name and version of software/segment>

<Document Version (if applicable)>

<Date>

Prepared for:

Defense Information Systems Agency

Table of Contents

<< GENERATE THE TABLE OF CONTENTS HERE >>

To generate the Table of Contents:

1. From the Insert menu select *Index* and *Tables*
2. Select the *Table of Contents* tab
3. Highlight *Custom Style* in the formats window, and the preview window will show the headings used
4. Click on "OK" to generate the Table of Contents

List of Tables

<< GENERATE THE LIST OF TABLES HERE >> .....

To generate the List of Tables:

1. From the Insert menu select *Index* and *Tables*
2. Select the *Table of Figures* tab
3. Highlight *Table* in the Caption Label window
4. Highlight *Custom Style* in the formats window, and the preview window will show the headings used
5. Click on "OK" to generate the List of Tables

List of Figures

<< GENERATE THE LIST OF FIGURES >>

To generate the List of Figures:

1. From the Insert menu select *Index* and *Tables*
2. Select the *Table of Figures* tab
3. Highlight *Figure* in the Caption Label window
4. Highlight *Custom Style* in the formats window, and the preview window will show the headings used
5. Click on "OK" to generate the List of Figures

Notes on Using the Template

1. Refer to Section 3.1 and 3.2 of the *DII COE Developer Documentation Requirements* for format requirements and guidelines for using the templates.
2. This template has been formatted for a small document (12 pages or less). Section headings are left adjusted (refer to Section 3.1.6 of the *DII COE Developer Documentation Requirements*) and are not required to begin on a new odd page.

1. SCOPE

This section shall be divided into the following paragraphs.

1.1 IDENTIFICATION

This paragraph shall contain a full identification of the system and the software. It must provide the name(s), title(s), abbreviation(s), version number(s), and the release number(s). Identification must include the operating system platform(s) to which this document applies.

1.2 System Overview

This paragraph shall provide a brief description of the general nature, purpose, and function of the system/software.

Provide references to additional information sources. Include documentation that may assist the user when problems are encountered. Identify each document by document number, title, version/revision, date, and source. Provide a point of contact to be used for reporting problems. Include facilities or organizations equipped to help in the event problems are encountered during installation. Identify organizations with mailing address, telephone number, fax number, and Web page or Internet address, as available.

2. Referenced Documents

Provide a list of documents referenced in this document. List each document by document number, title, version/revision, and date. Identify the source for all documents not available through the Government.

3. System Environment

Describe the system environment necessary to perform the installation of the software in this section. Include system and software configuration information, identify dependencies and compatibility issues, and provide any procedures that must be performed prior to installing the software.

3.1 System Requirements

3.1.1 Hardware Requirements

Identify all system hardware resources required to perform the software installation by name, number, type, size, etc. Provide the RAM and hard disk space required by the software/segment. Provide other requirements for computers, memory, drives, and other devices or components, as applicable.

3.1.2 Operating System Requirements

Identify the operating system and related components required to perform the software installation by names, version numbers, and release numbers, as applicable.

3.1.3 Kernel Requirements

Identify the DII COE Kernel version required to perform the software installation by name, version number, and release number, as applicable.

3.2 System and Site Preparations

Describe the system and site preparations that need to be performed prior to installing the software. Provide procedures for setting up the hardware and software, as needed. Identify hardware/software dependencies and exceptions to configuration, as applicable.

3.2.1 System Configuration

List any software or hardware components that must be installed and configured prior to the installation of the software (e.g., Telecom, Distributed Computing Environment (DCE), etc.). This section may cover requirements for upgrading specific system software with version dependencies.

3.2.2 Operating System Preparation

Provide procedures or information, if any, needed to prepare the operating system. Provide specific system requirements prior to installation (e.g., security, system privileges).

3.2.3 Tape/Disk Preparation

Provide procedures or information needed to prepare the tape or disk drive and related media, as applicable. Identify the physical media containing the software. Describe the disk partitioning and library set-ups that may be required.

4. Installation Instructions

Provide the step by step procedure and instructions for installing, configuring, and initializing the system software or segment into the appropriate libraries using the COE approved guidelines for segment installation and verification.

4.1 Media Booting Procedure

Provide instructions for booting the media containing the software, as needed, with specific options when required for the installation.

4.2 Installation Procedures

Provide the step by step procedures for configuring and installing the software. Provide instructions on how to load or download the software or segment into specific libraries using the DII COE approved guidelines for segment installation and verification.

4.3 Installation of Upgrades

Provide the step by step procedures and instructions for upgrading already installed software with new versions or patches. Identify the loading or downloading sequence and options for the software or segment installation.

4.4 Installation Verification

Describe procedures or a method (such as a checklist) for determining if the software installation was successful. This section may also describe and provide instructions for any software verification routines or programs provided, if any.

4.5 Initializing the Software

Describe the steps to be performed at the completion of the software installation. Include the procedures required for the initialization of system and software program operations.

4.6 List of Changes and Enhancements

Provide a brief description of the changes, enhancements, and fixes (patches) incorporated into this version of the software. Reference the applicable SVD for a detailed list of the software changes.

4.7 Important Considerations

Provide any security, licensing, privacy, and/or safety precautions and instruction relevant to the software being installed. This section may also provide critical back-up and archiving instruction.

5. Notes

Provide general information to assist in the understanding of this document. This section may include a list of acronyms and abbreviations, and a list of terms and definitions.

6. Documentation Improvement and Feedback

Comments and other feedback on this document should be directed to the DII COE Hotline:

Phone: 703-735-8681
Fax.: 703-735-3080
Email: HotlineC@ncr.disa.mil

A. Appendices

Appendices may be used to provide additional information published separately for convenience in document maintenance. The appendices shall be referenced in the main body of the document, where applicable.

G.4 Sample Test Script

This is an example of test cases and procedures used by the ISF to test the proper installation and functionality of the software.

Generating SQL Scripts for SMS Views

The information in this article applies to:

- Microsoft Systems Management Server 1.1
- Microsoft Systems Management Server 1.2

This article was previously published under Q133253

Summary

SMSVIEW creates various views that can be used when querying the Systems Management Server SQL Database. The SQL Scripts used to create these views can be dumped using Microsoft SQL Enterprise Manager (in Microsoft SQL Server 6.0).

More Information

To generate the SQL scripts to create the SMS views:

1. Start SQL Enterprise Manager.
2. If the server where the Systems Management Server database resides is not already registered in SQL Enterprise Manager, register it as follows:
    1. Select Register Server from the Server menu.
    2. Provide the server name and valid logon information (by default, the valid logon is SA with no password and Standard Security).
    3. Choose Register.
3. In the Server Manager window, select the server you just registered (there may be a slight delay as a connection to this server is established).
4. Choose in the following order:

    1. The Server's name in the Server Manager window.
    2. Databases to get to the Systems Management Server database.
    3. The database that contains the Systems Management Server data.

    The name of the SMS database in the Server Manager window should be selected.

5. Select Generate SQL Scripts from the Object menu.
6. In the Generate SQL Scripts - <servername>\<database name> dialog box, choose All Views for Scripting Objects. This fills in the name of each view in the list box at the bottom right portion of the dialog box.
7. Ensure Object Creation and Object Drop are selected for Scripting Options.
8. If you prefer scripts for each view to be placed in a separate file, select Per Object in Scripting Options. Otherwise, select Single File.

9. Choose Preview (there is a short wait as the scripts are generated). Save the scripts as text files or choose Close to go back to the Generate SQL Scripts dialog box without saving the scripts.

The following displays the resulting output (in Systems Management Server 1.1, Build 682):

```
/****** Object:  View dbo.vDisk    Script Date: 7/5/95 4:30:43 AM ******/
if exists (select * from sysobjects where id = object_id('dbo.vDisk') and
sysstat & 0xf = 2)
drop view dbo.vDisk
GO
Create View vDisk as select dwMachineID , Disk_SPEC.__Disk_Full0 ,
Disk_COMM.Disk_Index0 , Disk_COMM.File_System0 ,
Disk_SPEC.Free_Storage__MByte_0 , Disk_SPEC.Sectors0 ,
Disk_SPEC.Serial_Number0 , Disk_SPEC.Storage_Size__MByte_0 ,
Disk_COMM.Storage_Type0 , Disk_SPEC.Storage_Used__MByte_0 ,
Disk_SPEC.Volume_Name0 from  MachineDataTable  ,Disk_COMM   , Disk_SPEC
where Disk_COMM.datakey =*  CommonKey and Disk_SPEC.datakey =* SpecificKey
and ArchitectureKey = 5 and GroupKey = 8
GO
/****** Object:  View dbo.vEnvironment    Script Date: 7/5/95 4:30:43 AM
******/
if exists (select * from sysobjects where id =
object_id('dbo.vEnvironment')
and sysstat & 0xf = 2)
drop view dbo.vEnvironment
GO
Create View vEnvironment as select dwMachineID ,
Environment_SPEC.Environment_String0 , Environment_SPEC.Value0 from
MachineDataTable  ,Environment_COMM   , Environment_SPEC where
Environment_COMM.datakey =*  CommonKey and Environment_SPEC.datakey =*
SpecificKey and ArchitectureKey = 5 and GroupKey = 12
GO
/****** Object:  View dbo.vGroupNames    Script Date: 7/5/95 4:30:44 AM
******/
if exists (select * from sysobjects where id = object_id('dbo.vGroupNames')
and sysstat & 0xf = 2)
drop view dbo.vGroupNames
GO
Create View vGroupNames as select  GM.GroupName   FROM ArchitectureMap AM,
GroupMap GM  WHERE  GM.ArchitectureKey = AM.ArchitectureKey AND
((AM.Mode=0))
GO
/****** Object:  View dbo.vIdentification    Script Date: 7/5/95 4:30:44 AM
******/
if exists (select * from sysobjects where id =
```

```
object_id('dbo.vIdentification') and sysstat & 0xf = 2)
drop view dbo.vIdentification
GO
Create View vIdentification as select dwMachineID ,
Identification_SPEC.Domain0 , Identification_SPEC.LogOn_Name0 ,
Identification_SPEC.Name0 , Identification_SPEC.NetCardID0 ,
Identification_SPEC.Site0 , Identification_SPEC.SMSID0 ,
Identification_SPEC.SMSLocation0 , Identification_SPEC.SystemRole0 ,
Identification_SPEC.SystemType0 from  MachineDataTable
,Identification_COMM
, Identification_SPEC where Identification_COMM.datakey =*  CommonKey and
Identification_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and
GroupKey = 1
GO
/****** Object:  View dbo.vMouse    Script Date: 7/5/95 4:30:44 AM ******/
if exists (select * from sysobjects where id = object_id('dbo.vMouse') and
sysstat & 0xf = 2)
drop view dbo.vMouse
GO
Create View vMouse as select dwMachineID , Mouse_COMM.Hardware_Installed0 ,
Mouse_COMM.Language0 , Mouse_COMM.Manufacturer0 ,
Mouse_COMM.Mouse_Hardware_Type0 , Mouse_COMM.Number_of_Buttons0 from
MachineDataTable  ,Mouse_COMM   , Mouse_SPEC where Mouse_COMM.datakey =*
CommonKey and Mouse_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and
GroupKey = 4
GO
/****** Object:  View dbo.vNetcard    Script Date: 7/5/95 4:30:45 AM
******/
if exists (select * from sysobjects where id = object_id('dbo.vNetcard')
and
sysstat & 0xf = 2) drop view dbo.vNetcard
GO
Create View vNetcard as select dwMachineID , Netcard_SPEC.IRQ0 ,
Netcard_COMM.Manufacturer0 , Netcard_SPEC.Port_Address0 from
MachineDataTable  ,Netcard_COMM   , Netcard_SPEC where Netcard_COMM.datakey
=*  CommonKey and Netcard_SPEC.datakey =* SpecificKey and ArchitectureKey =
5 and GroupKey = 11
GO
/****** Object:  View dbo.vNetwork    Script Date: 7/5/95 4:30:45 AM
******/
if exists (select * from sysobjects where id = object_id('dbo.vNetwork')
and
sysstat & 0xf = 2) drop view dbo.vNetwork
GO
Create View vNetwork as select dwMachineID , Network_COMM.Default_Gateway0
Network_SPEC.IP_Address0 , Network_SPEC.IPX_Address0 ,
```

```
Network_COMM.LogOn_Name0 , Network_COMM.Major_Version0 ,
Network_COMM.Minor_Version0 , Network_SPEC.Network_Active0 ,
Network_COMM.Network_Type0 , Network_COMM.Subnet_Mask0 from
MachineDataTable  ,Network_COMM   , Network_SPEC where Network_COMM.datakey
=*  CommonKey and Network_SPEC.datakey =* SpecificKey and ArchitectureKey =
5 and GroupKey = 10
GO
/****** Object:  View dbo.vOperating_System    Script Date: 7/5/95 4:30:45
AM ******/
if exists (select * from sysobjects where id =
object_id('dbo.vOperating_System') and sysstat & 0xf = 2)
drop view dbo.vOperating_System
GO
Create View vOperating_System as select dwMachineID ,
Operating_System_COMM.Build_Number0 , Operating_System_COMM.Build_Type0 ,
Operating_System_COMM.Country_Code0 ,
Operating_System_SPEC.Installation_Date0 ,
Operating_System_COMM.Language_ID0 ,
Operating_System_COMM.Operating_System_Name0 ,
Operating_System_COMM.Registered_Organization0 ,
Operating_System_SPEC.Registered_Owner0 ,
Operating_System_SPEC.System_Root0
, Operating_System_SPEC.System_Start_Options0 ,
Operating_System_COMM.Version0 from  MachineDataTable
,Operating_System_COMM   , Operating_System_SPEC where
Operating_System_COMM.datakey =*  CommonKey and
Operating_System_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and
GroupKey = 7
GO
/****** Object:  View dbo.vPC_Memory    Script Date: 7/5/95 4:30:46 AM
******/
if exists (select * from sysobjects where id = object_id('dbo.vPC_Memory')
and sysstat & 0xf = 2)
drop view dbo.vPC_Memory
GO
Create View vPC_Memory as select dwMachineID ,
PC_Memory_SPEC.Page_File_Name0 , PC_Memory_SPEC.Page_File_Size__MByte_0 ,
PC_Memory_SPEC.Total_Paging_File_Space__0 ,
PC_Memory_SPEC.Total_Physical_Memory__KB0 from  MachineDataTable
,PC_Memory_COMM   , PC_Memory_SPEC where PC_Memory_COMM.datakey =*
CommonKey and PC_Memory_SPEC.datakey =* SpecificKey and ArchitectureKey = 5
and GroupKey = 9
GO
/****** Object:  View dbo.vProcessor    Script Date: 7/5/95 4:30:46 AM
******/
if exists (select * from sysobjects where id = object_id('dbo.vProcessor')
```

```
and sysstat & 0xf = 2)
drop view dbo.vProcessor
GO
Create View vProcessor as select dwMachineID ,
Processor_COMM.Processor_Name0 , Processor_COMM.Processor_Type0 ,
Processor_COMM.Quantity0 from  MachineDataTable  ,Processor_COMM   ,
Processor_SPEC where Processor_COMM.datakey =*  CommonKey and
Processor_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and
GroupKey = 6
GO
/****** Object:  View dbo.vServices    Script Date: 7/5/95 4:30:46 AM
******/
if exists (select * from sysobjects where id = object_id('dbo.vServices')
and sysstat & 0xf = 2)
drop view dbo.vServices
GO
Create View vServices as select dwMachineID , Services_SPEC.EXE_Path0 ,
Services_COMM.Name0 , Services_SPEC.Start_Name0 , Services_COMM.Start_Type0
, Services_COMM.State0 from  MachineDataTable  ,Services_COMM   ,
Services_SPEC where Services_COMM.datakey =*  CommonKey and
Services_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and
GroupKey = 13
GO
/****** Object:  View dbo.vVideo    Script Date: 7/5/95 4:30:47 AM ******/
if exists (select * from sysobjects where id = object_id('dbo.vVideo') and
sysstat & 0xf = 2)
drop view dbo.vVideo
GO
Create View vVideo as select dwMachineID , Video_COMM._nd_Adapter_Type0 ,
Video_COMM.Adapter_Type0 , Video_SPEC.Bios_Date0 ,
Video_COMM.Current_Video_Mode0 , Video_COMM.Display_Type0 ,
Video_COMM.Manufacturer0 , Video_COMM.Max_Rows0 from  MachineDataTable
,Video_COMM   , Video_SPEC where Video_COMM.datakey =*  CommonKey and
Video_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and GroupKey = 5
GO
/****** Object:  View dbo.vWorkstationStatus    Script Date: 7/5/95 4:30:47
AM ******/
if exists (select * from sysobjects where id =
object_id('dbo.vWorkstationStatus') and sysstat & 0xf = 2)
drop view dbo.vWorkstationStatus
GO
Create View vWorkstationStatus as select dwMachineID ,
WorkstationStatus.Failed_Hardware_Checks0 ,
WorkstationStatus.Files_Not_Installed0 , WorkstationStatus.LastHWScan ,
WorkstationStatus.LastSWScan , WorkstationStatus.Standalone_Workstation0 ,
WorkstationStatus.System_Files_Not_Modified0 from  MachineDataTable  ,
```

```
WorkstationStatus where WorkstationStatus.datakey =* SpecificKey and
ArchitectureKey = 5 and GroupKey = 2
GO
```

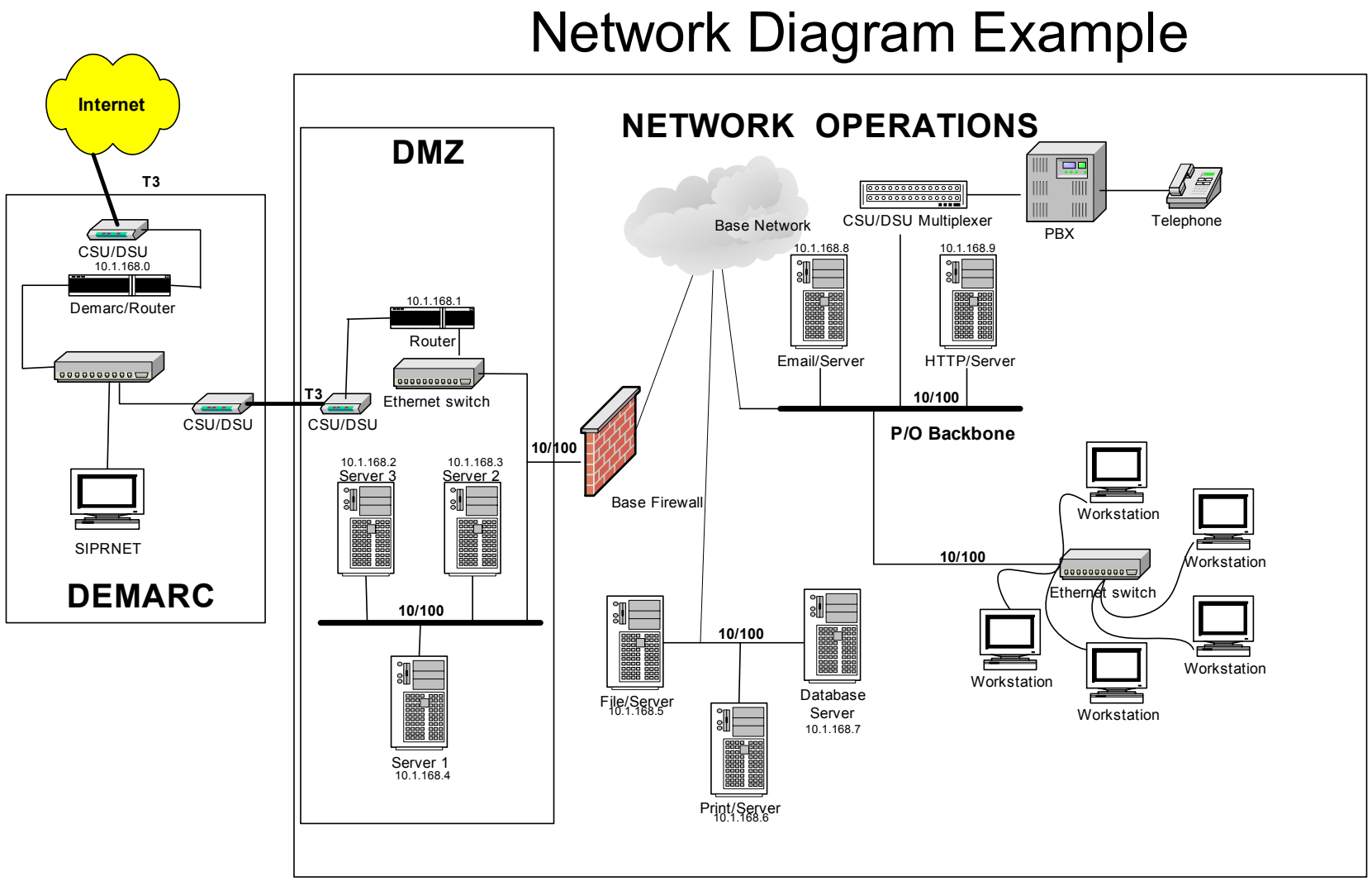
G.5 UTAM Template

UTAM Master Template

Site:
Date:
POC:
Address:
PhoneNumber:
Email:

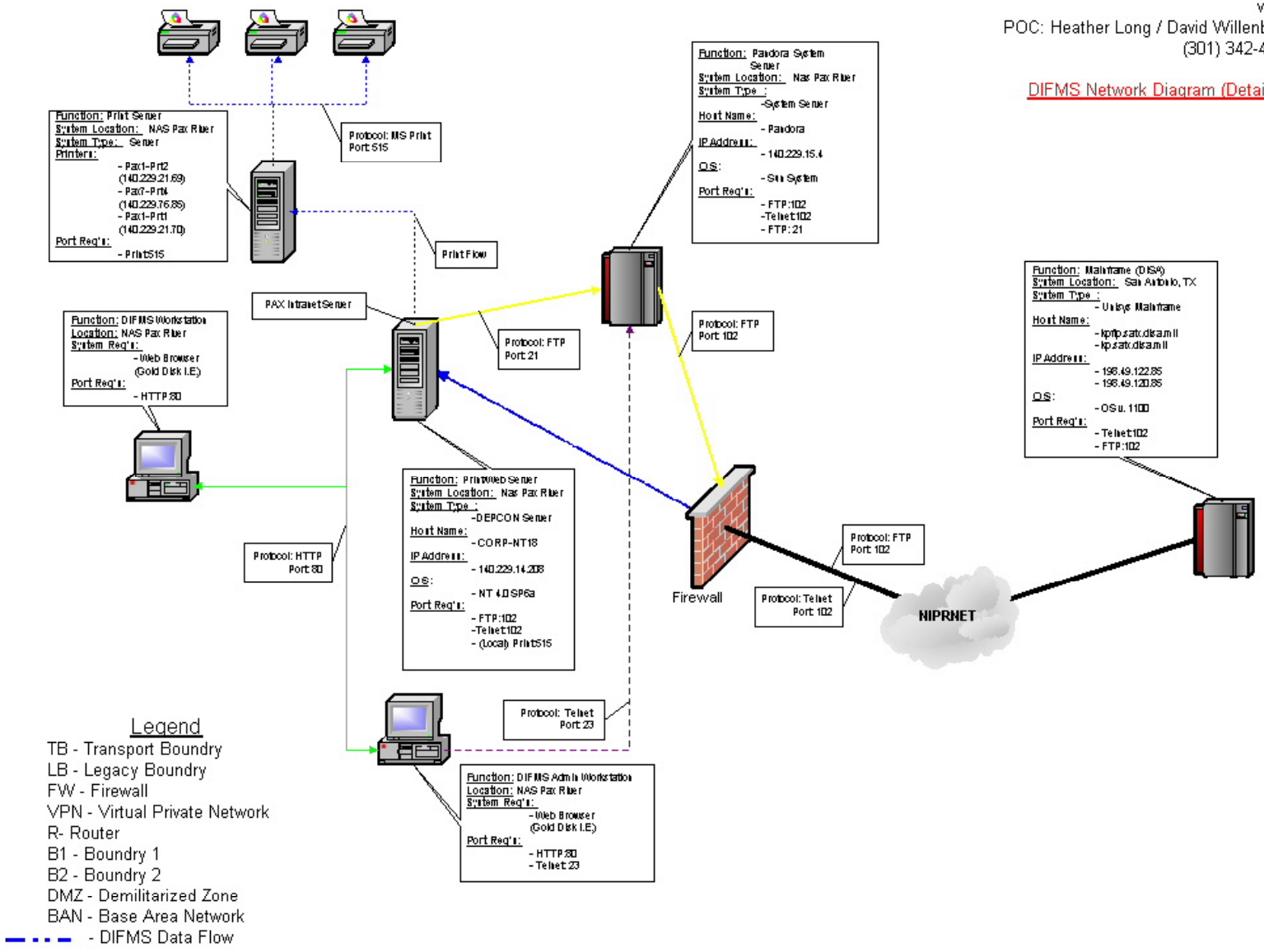
Application Name	NOVADIGM Application Name	RFS	Last Name	First Name	Middle Initial	User Name	Domain	NetID
Microsoft Word		100	Doe	Joe	E	joe.e.doe.@test.com	cmdhq	doej
			Smith	Jane	A	jane.a.smith@test.com	cmdhq	smithj
			Williams	Will	B	will.b.williams@resource.com	fincmdhq	williamsw
Microsoft Excel		115	Doe	Joe	E	joe.e.doe.@test.com	cmdhq	doej
			Smith	Jane	A	jane.a.smith@test.com	cmdhq	smithj
			Williams	Will	B	will.b.williams@resource.com	fincmdhq	williamsw
Power Point		117	Doe	Joe	E	joe.e.doe.@test.com	cmdhq	doej
			Smith	Jane	A	jane.a.smith@test.com	cmdhq	smithj
			Williams	Will	B	will.b.williams@resource.com	fincmdhq	williamsw
Visio 2000		110	Doe	Joe	E	joe.e.doe.@test.com	cmdhq	doej
			Smith	Jane	A	jane.a.smith@test.com	cmdhq	smithj
			Williams	Will	B	will.b.williams@resource.com	fincmdhq	williamsw

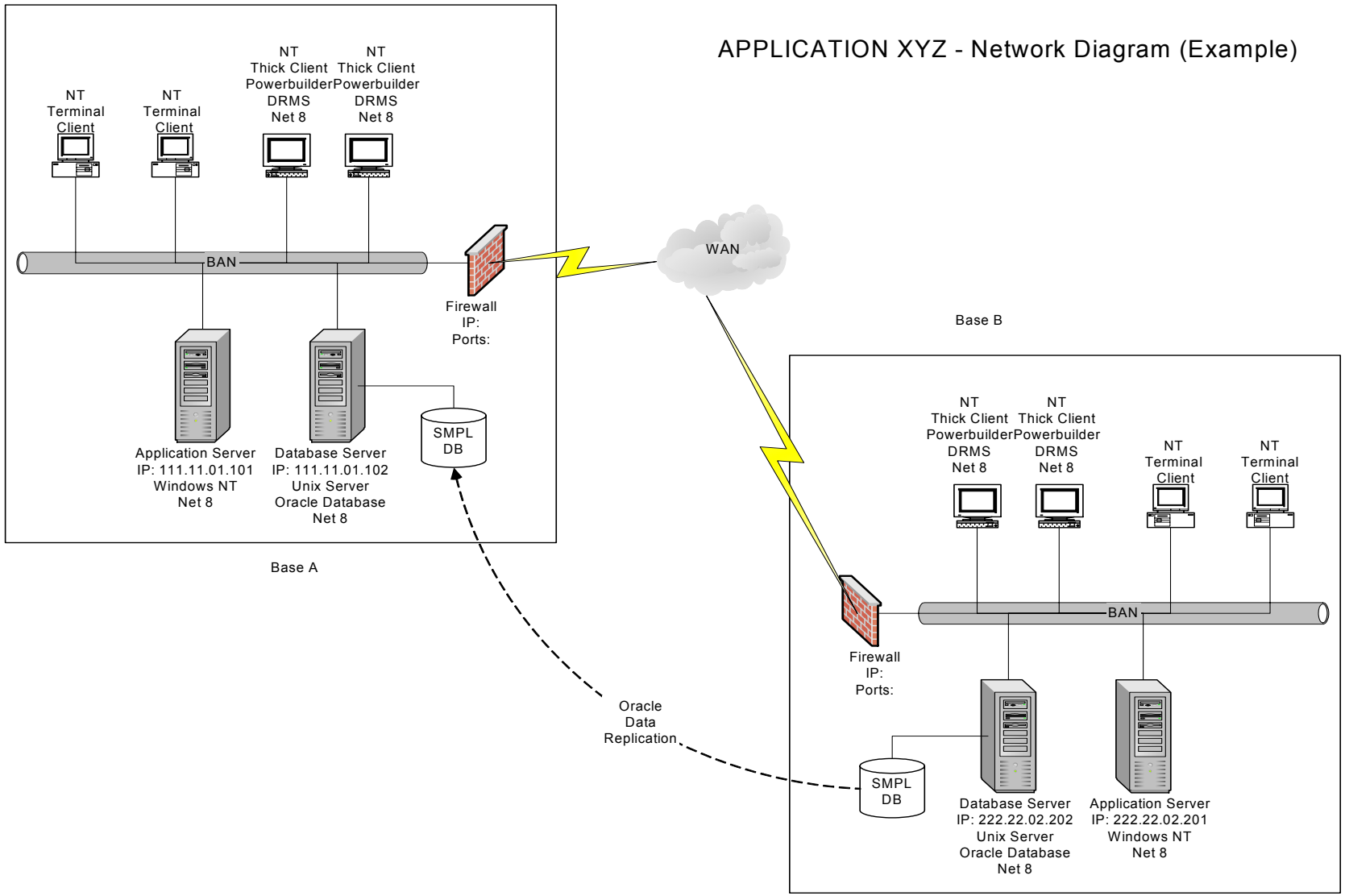
G.6 Network Diagram Examples



RFS: 2274
Defense Industrial Financial Management System (DIFMS)
v.00A
POC: Heather Long / David Willenborg
(301) 342-4621

DIFMS Network Diagram (Detailed)




APPLICATION XYZ - Network Diagram (Example)
NT Terminal Client
NT Terminal Client
NT Thick Client Powerbuilder DRMS Net 8
NT Thick Client Powerbuilder DRMS Net 8
BAN
Firewall IP: Ports:
WAN
Application Server IP: 111.11.01.101 Windows NT Net 8
Database Server IP: 111.11.01.102 Unix Server Oracle Database Net 8
SMPL DB
Base A
Base B
NT Thick Client Powerbuilder DRMS Net 8
NT Thick Client Powerbuilder DRMS Net 8
NT Terminal Client
NT Terminal Client
BAN
Firewall IP: Ports:
Oracle Data Replication
SMPL DB
Database Server IP: 222.22.02.202 Unix Server Oracle Database Net 8
Application Server IP: 222.22.02.201 Windows NT Net 8

G.7 Reachback and Datashare

Datashare/Reachback

Client		Datashare resources							Reachback						
User Name	Domain	Mapped Drives and Devices	Device or Service Name	Port	Protocol	IP Address	POC	Phone#	Desktop Name	IP	Router 1 IP	Router 2 IP	Router n... IP	Destination Name	IP
		1													
		2													
		3													
		4													
		Peripherals													
		Printers													
		Scanners													
		Other													
		Local Network Connections													
		Database													
		Server													
		Library													
		Peripheral													
		Other													
		Outer Network Connections													

Client		Datashare resources							Reachback						
User Name	Domain	Mapped Drives and Devices	Device or Service Name	Port	Protocol	IP Address	POC	Phone#	Desktop Name	IP	Router 1 IP	Router 2 IP	Router n... IP	Destination Name	IP
		1													
		2													
		3													
		4													
		Peripherals													
		Printers													
		Scanners													
		Other													
		Local Network Connections													
		Database													
		Server													
		Library													
		Peripheral													
		Other													
		Outer Network Connections													

G.8 Legacy Server Template

Legacy Server Template

Site: _____
Date: _____
POC: _____
Address: _____
_____
PhoneNumber: _____
Email: _____

Line#	Serial Number	Name Server	Net Bios Name	IP Address	Gateway Address	Protocol	Domain Name	Fully Qualified Domin Name	Server Type	MAC Address	Operating System	Application Name	Version Number	Bus Type	Server Resources

Legacy Server Template Definitions

Line Number*	Sequential listing of assign assets (1,2,3...)
Serial Number*	The server's physical identification number
Name Server*	The unique name specifying a given path to the server's resources (ex. NCC.NCTS.NAVY.MIL)
NetBios Name*	Also called the computer name. The physical name of the server (ex. "finance", "cost analysis") note: 1) LMHost file contains mappings of IP Address to NetBios (computernames) i.e. 156.27.168.5 "Finance" 2) The Host file contains mappings of IP Addresses to Host Names i.e. 156.27.168.0 "finance. NAVY.MIL"
IP Address*	An identifier (name) for a computer or device on a TCP/IP network. The Servers logical address i.e. "172.68.156.5"
Gateway Address*	A node on a network that serves as an entrance to another network. The logical address of the intended network usually associated with a router i.e. "172. 16. 168.0"
Protocol*	Identify the internetworking protocol employed by the server
Domain Name*	A name which identifies one or more IP Address (navy.mil, ucla.edu, microsoft.com)
Fully Qualified Domain Name	(FQDN) A DNS domain name that has been stated unambiguously so as to indicate with absolute certainty its location in the domain namespace tree. Fully qualified domain names differ from relative names in that they are typically stated with a trailing period (.) - for example, host.example.microsoft.com. - to qualify their position to the root of the namespace. Locally, you can find the FQDN by running a trace route "tracert" on it's IP address.
Server Type*	Identify the general/overall function of the server
MAC Address*	Media Access Control Address: A hardware address which uniquely identifies a device on the network. The hardware address of a device connected to a shared network. Ex. It is the physical address of the server's NIC Card
Operating System*	The software platform on top of which all application programs run (i.e. Windows 95,98,NT,Unix)
Application Name*	List all application residing on the server
Version Number*	List the version number of each application
Bus Type*	List the bus specification for each application (i.e. 8,16,32 bit)
Server Resources	List all associated and miscellaneous applications residing on the server

* mandatory item

Appendix H — Enterprise B1, B2, and GPO and Operational Management

This appendix shows where B1 and B2 are implemented. Each boundary serves a purpose. The Boundary 1 (NOC) protects access to NIPRNet and Internet. The Boundary 2 performs similar functions as B1, except that the rules are more permissive for an interface with existing internal Navy and USMC networks.

Boundary Protection

Boundary Protections are the standard sets of protections that define the interfaces within NMCI and between NMCI and other networks. See Figure H-1 below. Boundary Protections enforce the policies required to connect to those external networks, provide security mechanisms for secure access to applications, and protect communities of interest (COIs) residing within NMCI. The type and strength of each security component is dependent upon the information protection requirements for a particular DON system. This is especially true for boundaries 1, 2 and 3. Boundary 1 reflects the Navy Marine Corps Enclave Protection Policy. Boundaries 2 and 3 security mechanisms are flexible enough to meet the security requirements of various scenarios. Specific configuration parameters of the security components deployed at the various boundary levels are tailored to provide the level of protection necessary to protect the confidentiality, integrity and availability, accountability and non-repudiation of NMCI.

GPO Overview

Group Policy is an Active Directory-based mechanism for controlling user and computer desktop environments in Windows 2000 domains. Settings for such items as security, software installation, and scripts can be specified through Group Policy. Group Policies are very simple to implement but can be quite complex to configure. Each GPO can consist of two parts: one that applies to a computer and one that applies to a user. GPOs can contain only computer policies, only user policies, or a mixture of the two. Group Policy is applied to groups of users and computers based on their location in the Active Directory. Group Policy allows the administrator to stipulate users' environments only once, and then rely on the operating system to enforce them thereafter.

Group Policy objects are not profiles. Profiles are user environment settings and are configurable by the user. Policies are standards configured by the administrator that are applied during computer boot-up and user log-on. They specify system behavior and restrict what users are allowed to do. Local policies are stored locally, within the computer's registry. Non-local policies are stored in the Active Directory. Local policies are not configured within the NMCI environment.

Group Policies are processed first at the site level, then the domain level, and finally at the organizational unit (OU) level. The administratively specified order determines the Group Policy settings that a user or computer actually receives. Furthermore, policy can be blocked at the Active Directory domain, or OU level.

Following are NMCI Group Policies:
Account policies are applied at the NADSUSWE, NADSUSEA, MADSUS, and NMCI domains.
User and computer policies are applied at the Command level OUs and below.
Domain Controller policies are applied at the Domain Controller OU.
Server policies are applied at the Application Services OU and below.
Login script policies are applied where applicable.
Workstation preference policies are applied at the Command level OUs.

Enterprise-wide permissions, parent to child domain (i.e., NADS to NADSUSWE) and domain to domain (i.e., NADSUSEA to NADSUSWE), and Group Policy propagation of permissions and traffic will exist but these practices will be scrutinized for performance issues.

Group Policy provides the following advantages:

Integration with Windows 2000 Active Directory services
Flexibility and scalability
Provides an integrated tool for managing policy (MMC snap-in)
Consistent and easy to use GPO snap-in
Reliability and security

Operational Management

B1 Operational Management consists of the Office of the CNO (OPNAV N614) approving a common Enterprise Policy and ISF managing a policy-compliant operational configuration. To do this, ISF IA receives PIAB/LDSD&T trace data and recommends policy compliant Rulesets. ISF IA manages the Ruleset release, monitors implementation, and manages any legacy applications IA problems. ISF IA engineering develops policy-compliant firewall Rulesets. ISF IA then configures B1 firewall to include the released Rulesets. Finally, Wam!Net configures B1 router Access Control Lists (ACL) to duplicate firewall Rulesets. Figure I-3 shows the Boundary 1 Architecture.

B2 Operational Management consists of NETWARCOM approving a common Enterprise Policy and ISF managing a policy-compliant operational configuration. To do this, ISF IA develops policy-compliant Rulesets, receives PIAB/LDSD&T trace data and develops ACL mitigation rules. ISF IA manages the mitigation Ruleset release, monitors implementation, and manages any legacy applications IA problems. ISF IA also recommends common enterprise policy changes to NETWARCOM. ISF IA Transition configures B2 firewall to conform to the released common firewall Rulesets. Finally, Wam!Net configures B2 router ACLs to conform to released mitigation Ruleset. Figure I-4 shows the Boundary 2 Architecture.

GPO Operational Management involves NETWARCOM approving a common Enterprise Policy. This policy is known as WorkstationSEC (security). ISF IA reviews WorkstationSEC GPO rules and approves its release. ISF IA manages the policy-compliant operational configuration. ISF IA develops policy compliant GPO Rulesets, conducts vulnerability tests and issues Risk Assessment Reports. ISF IA also manages mitigation Ruleset release and recommends common enterprise policy changes to NETWARCOM. The NOC staff applies the Enterprise GPO to the Active Directory. GPO then replicates down to workstations throughout NMCI.

Figure H-1. Boundary Interfaces

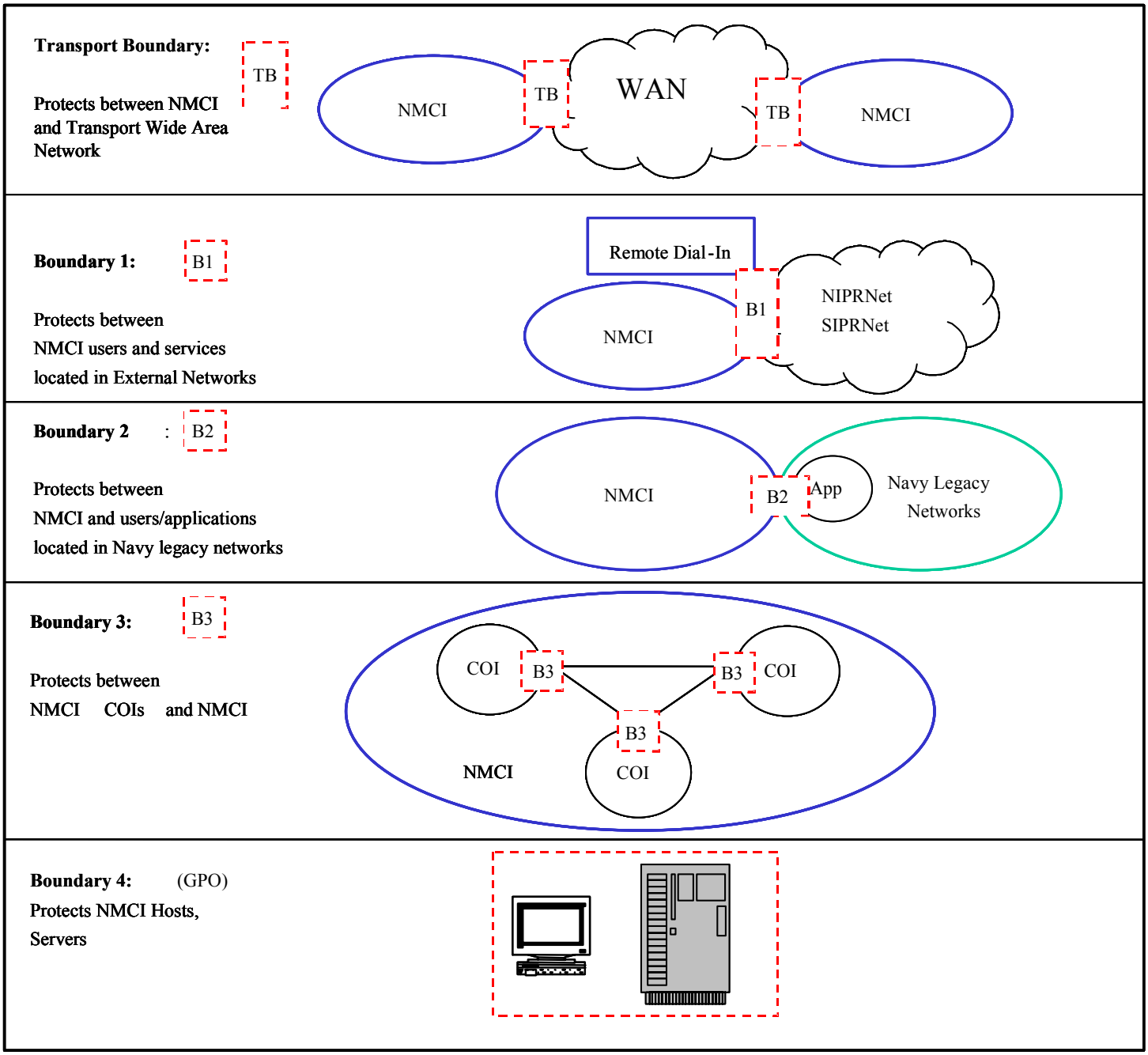


Figure H2. Simplified NMCI Architecture Overview

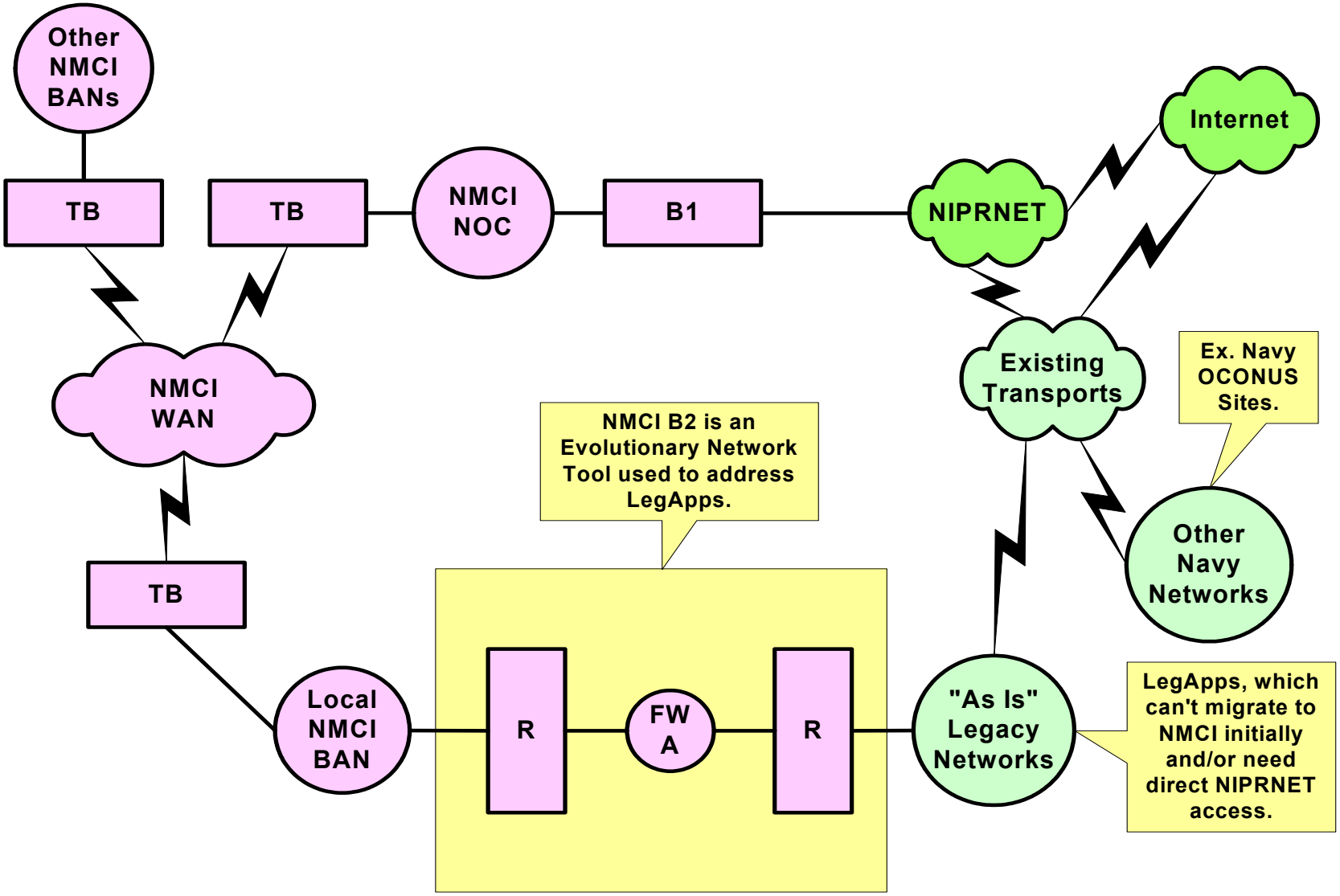


Figure H-3. Boundary 1 Architecture

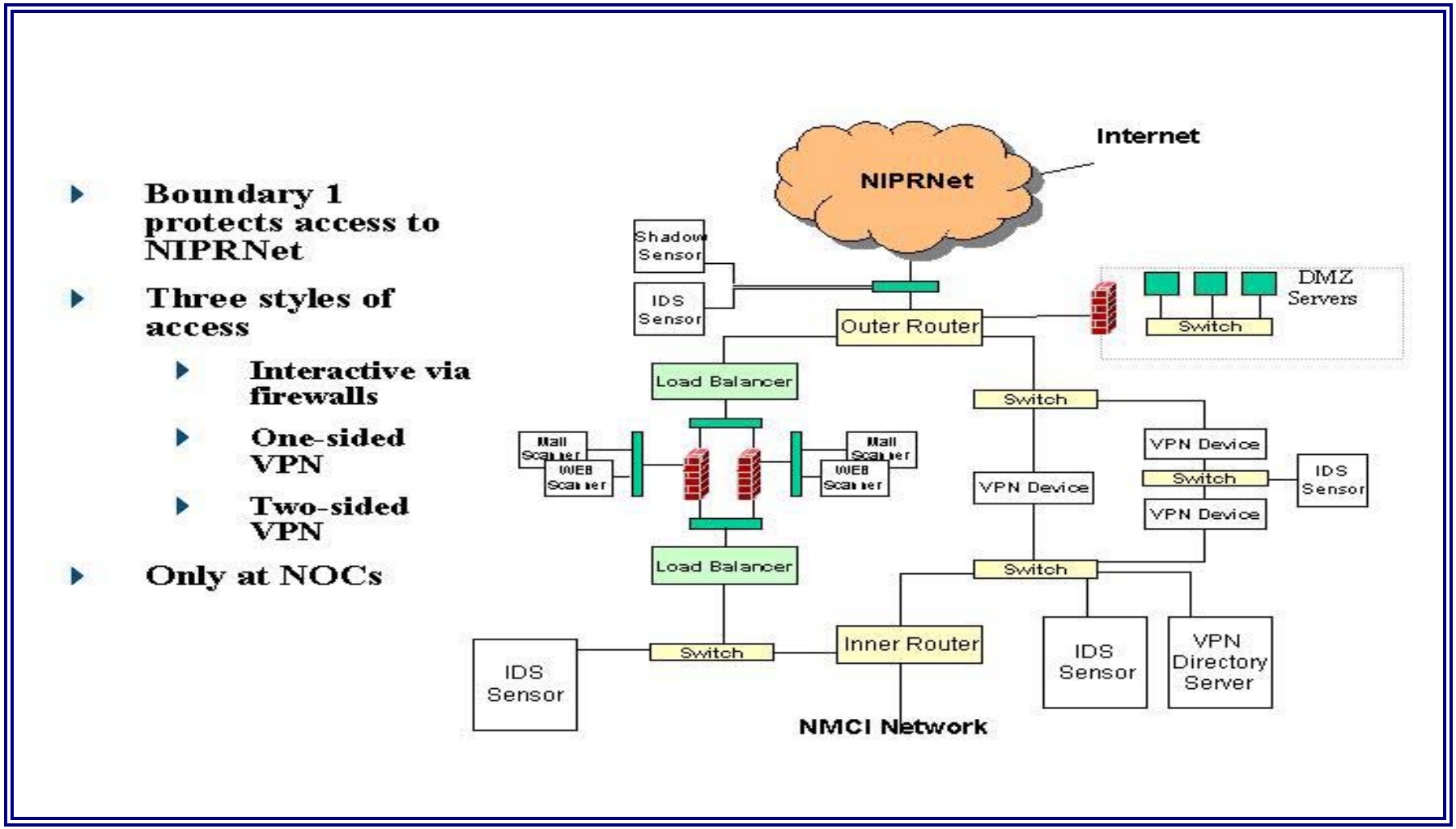
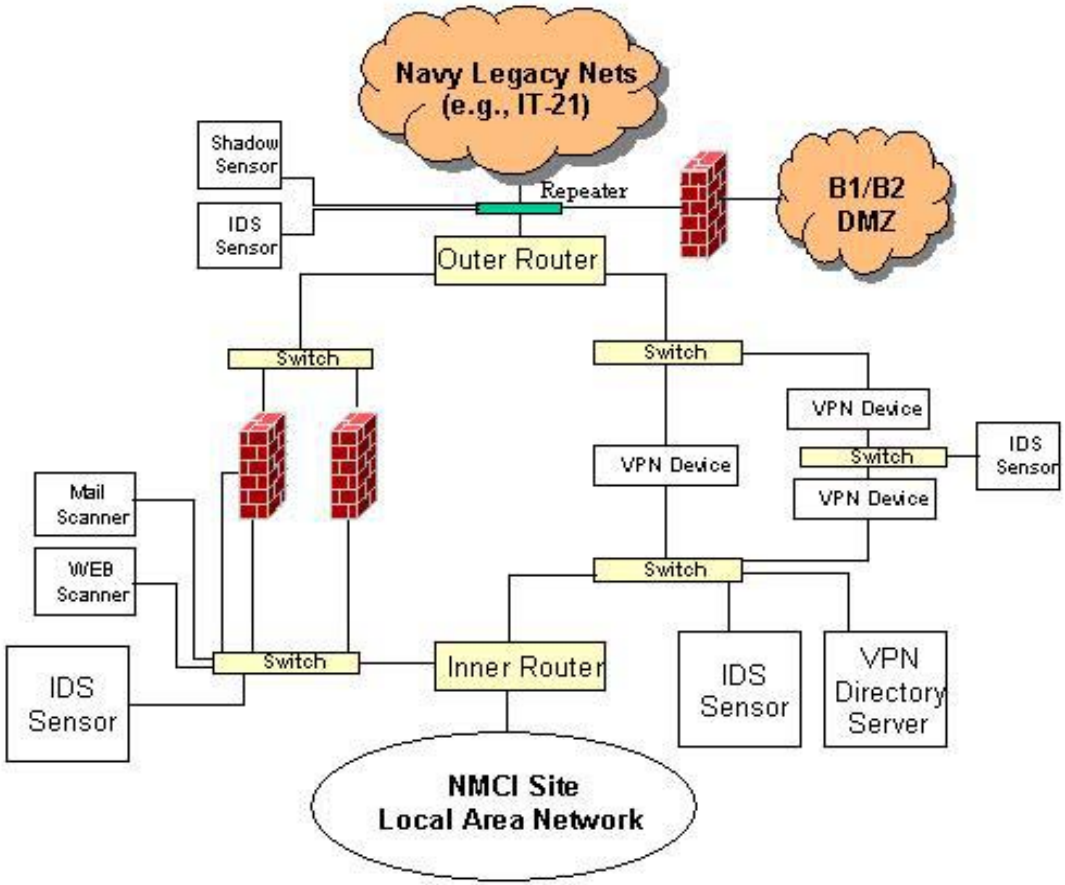


Figure H-4. Boundary 2 Architecture

- **Interface to internal Navy and USMC networks**
- **Employed at sites and NOCs**
- **Same architecture as Boundary 1**
- **Allows separate policy vice Boundary 1**



Appendix I — Glossary

Access: The availability of the full functionality of a system/application at the end-user desktop.

Accreditation: Formal declaration by a Designated Approval Authority (DAA) that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. *Source: National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4009, National Information Systems Security (INFOSEC) Glossary.*

Agent Software: Any software that monitors and/or captures network traffic or queries network nodes for the purpose of reporting the captured information back to the user or another network node. This type of information is considered sensitive and its capture and dissemination poses a security risk.

Alpha Testing: A very early version of a software product that may not contain all of the features that are planned for the final version. Typically, software goes through two stages of testing before it is considered finished. Often, only users within the organization developing the software perform the first stage, called alpha testing. The second stage, called *beta testing*, generally involves a limited number of external users.

Application: (1) An automated software program that collects, stores, processes, and/or reports information in support of a specific user requirement. (2) Any software program that runs in a server-based or stand-alone environment that is used in a production capacity.

Application Development Software: Any software that generates or allows the user to create programming code which complies into executable (.exe) files that are installed and can be run from the user's workstation. Application Development Software is only permitted to reside on S&T seats.

Application survey: The process of gathering COTS and GOTS application information necessary to rationalize or certify applications for migration to the NMCI environment. There are three categories of applications surveys: (1) desktop – a single user application not on the standard NMCI seat, (2) server-based, and (3) Web-based.

Assumption of Responsibility (AOR): The date when responsibility for operating the "as-is" environment and for work defined by the ordered NMCI CLINs shifts from the government and its local contractors to the Information Strike Force.

Beta Test: A test for a computer product prior to commercial release. Beta testing is the last stage of testing, and normally involves sending the product to *beta test sites* outside the company for real-world exposure. A round of testing called alpha testing often precedes beta testing.

Certification: The act of functionally testing an application for compatibility with the NMCI environment. This includes testing for Windows 2000 compatibility, Gold Disk interoperability, and GPO compliance, as well as compliance with Navy Boundary Policies. The NMCI Ruleset is enforced by the ISF at the time of certification testing.

Certification and Accreditation (C&A): The comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. *Source: National Security Telecommunications and Information*

Systems Security Instruction (NSTISSI) 4009, National Information Systems Security (INFOSEC) Glossary. Includes testing the ability of the application to electronically distribute.

Client: The client part of *client-server architecture*. Typically, a client is an application that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an *e-mail client* is an application that enables you to send and receive e-mail.

Client-Server Architecture: A network architecture in which each computer or process on the network is either a *client* or a *server*. Servers are powerful computers or processes dedicated to managing disk drives (*file servers*), printers (*print servers*), or network traffic (*network servers)*. Clients are PCs or workstations on which users run applications. Clients rely on servers for resources, such as files, devices, and even processing power.

Connectivity: The establishment and maintenance of a connection between two or more points in the NMCI. Categories of connectivity include:

> Complex connectivity: Intranet connectivity involving systems/applications traversing protection boundaries internal to NMCI, but not Boundary 1, and extranet connectivity involving systems/ applications traversing NMCI boundaries, including Boundary 1, going external to NMCI.
>
> Simple connectivity: Local area connections involving systems/applications that are active within a local area only and do not traverse internal or external NMCI boundaries.

Cutover: The actual event of rolling out NMCI desktops. Cutover follows the preparation phases pre-AOR and post-AOR of the legacy applications transition.

> Cutover Start: In theory, Cutover begins at the pre-designated time when all pre-Cutover transition work is complete. Cutover actually begins upon the rollout of the first NMCI desktop at a site.
>
> Cutover Complete: In theory, Cutover is complete when the final desktop and application is successfully deployed. In actuality, Cutover ends at the successful rollout of the last scheduled desktop.

Deployment: The delivery of an authorized application to a designated server or desktop through an automated or local deployment process.

Driver: Drivers are the associated software designed to allow peripherals to function with the workstation/desktop. They are defined as:

- Software that interfaces with a computer to a specific peripheral.
- A device driver is a program that controls a particular type of device that is attached to your computer. They are device drivers for printers, displays, CD-ROM readers, diskette drives, and so on. A device driver essentially converts the more general input/output instructions of the operating system to messages that the device type can understand.

Enterprise: Literally, a business organization. In the computer industry, the term is often used to describe any large organization that utilizes computers. An intranet, for example, is a good example of an enterprise computing system. In this case, the entire NMCI environment.

Freeware: Copyrighted software given away for free by the author. Although it is available for free, the author retains the copyright, which means that one cannot do anything with it that is not expressly allowed by the author. Usually, the author allows people to use the software, but not sell it. Freeware is allowed in NMCI with approval of the FAM and NADTF.

Gameplan: The strategy devised before or used during an event. A strategy for reaching an objective. For NMCI, the Identification and Rationalization Gameplan is created to build the strategy a site will use to identify and rationalize their Legacy Applications.

Group Policy Object (GPO): a collection of settings that define what a system will look like and how it will behave for a defined group of users. GPO is associated with selected Active Directory containers, such as sites, domains, or organizational units (OUs).

Kernel: The central module of an operating system. It is the part of the operating system that loads first, and it remains in main memory. Because it stays in memory, it is important for the kernel to be as small as possible while still providing all the essential services required by other parts of the operating system and applications. Typically, the kernel is responsible for memory management, process and task management, and disk management.

Legacy Application: An existing customer software application that is not included in the NMCI standard seat services or the CLIN 0023 catalog.

Local Deployment: The act of manually loading an authorized client application to the NMCI seat.

Mapping: To make logical connections between two entities. Within NMCI, mapping is primarily related to a connection to an Active Directory Object enabling access to applications, data, and peripherals. Mapping is also used within NMCI to associate users, applications, and peripherals to desktops/workstations.

Media: Objects on which data can be stored. These include hard disks, floppy disks, CD-ROMs, and tapes.

Metadata: Data about data. Metadata describes how and when and by whom a particular set of data was collected, and how the data is formatted. Metadata is essential for understanding information stored in data warehouses.

Migration: The process of moving from the use of one operating environment to another operating environment. For NMCI, this means moving from the existing network (legacy) to NMCI.

Mission-Critical System: A system handling information determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of content and timeliness. It must be absolutely accurate and available on demand (may include classified information in a traditional context, as well as sensitive and unclassified information). *Source: Navy IA Publication 5239-1*. Mission-critical systems are categorized as follows:

> Category 1: Defined by the Clinger/Cohen Act as National Security Systems (NSS) (intelligence activities; cryptologic activities related to national security; Command and control of military forces, integral to a weapon or weapons system; systems critical to direct fulfillment of military or intelligence missions).

Category 2: In direct support of those systems identified by the Commanders in Chief (CINCs) which, if not functional, would preclude the CINC from conducting missions across the full spectrum of operations.

Category 3: Required to perform department-level and component-level core functions, including mission support.

NMCI Test Seat: An engineering tool used by ISF to test applications for compatibility with the NMCI environment. NMCI Test Seats are used when the NMCI infrastructure is in place and the end-to-end connectivity can be tested.

Peripheral: A computer device, such as a CD-ROM drive or printer, which is not part of the essential computer, i.e., the memory and microprocessor.

Point of Presence-In-A-Box (PoP-in-a-Box): An engineering tool used by ISF to test applications for compatibility with the NMCI environment. The PoP simulates the NMCI environment and consists of Windows 2000 operating system, servers, and routers.

Push: The act of centrally managing and distributing authorized client software to the NMCI seat. In NMCI, this is accomplished through the use of Novadigm Radia. The Novadigm Radia Instance is loaded to the NMCI seat through an automated process called "push".

Quarantine: A Quarantined application is one that is not allowed to operate in the NMCI environment. Applications that are Quarantined are left to operate in the Legacy environment. Reasons for an application being Quarantined include that the application may not function in Win2K, it may interfere with the Gold Disk, it may violate GPO/B1/B2 policies, it may violate NMCI Ruleset, it may have been identified/submitted too late to process, it may have no user/tester support, or it may have a network connectivity error.

Rationalization: The process of identifying only those desktop and server-based applications, both COTS and GOTS, required to support Command or DON missions and goals. It includes the integration, consolidation, and elimination of applications and databases to improve standardization, enhance security, reduce duplication, and minimize support costs.

Repository: A secure place where information is stored for safekeeping.

Script: Another term for *macro* or batch file, a script is a list of Commands that can be executed without user interaction. A *script language* is a simple programming language with which you can write scripts. For the Rapid Certification Phase, this refers to a "test script" used by the AIT lab to verify functionality of the application during testing.

Server: A computer or device on a network that manages network resources. For example, a *file server* is a computer and storage device dedicated to storing files.

Shareware: Software distributed on the basis of an honor system. Most shareware is delivered free of charge, but the author usually requests that one pay a small fee if one likes the program and uses it regularly. By sending the small fee, one becomes registered with the producer so that one can receive service assistance and updates. One can copy shareware and pass it along to friends and colleagues, but one must pay a fee if they use the product. According to the NMCI Ruleset, shareware is not authorized to operate in the NMCI environment.

System: (1) A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. *Source: Section 3502, Title 44, U.S. Code*.
(2) A group of interrelated and interdependent components, including applications, hardware, databases, and business procedures that, when combined, forms an organic whole and enables one or more functions.

SQL: Abbreviation of *structured query language*, and pronounced either *see-kwell* or as separate letters. SQL is a standardized query language for requesting information from a database.

URL: Abbreviation of *Uniform Resource Locator,* the global address of documents and other resources on the World Wide Web.

Appendix J — Acronym List

ACTR	Assistant Customer Technical Representative
ADS	Application Deployment Solution
AIS	Automated Information Systems
AIT	Application Integration and Testing
AOR	Assumption of Responsibility
ASNRDA	Assistant Secretary of the Navy for Research Development and Acquisition
ATO	Authority To Operate
B1	Boundary One
B2	Boundary Two
BLII	Base Level Information Infrastructure
CBA	Certification By Association
CDA	Central Design Authority/Central Design Activity/Central Development Activity
CIAT	Classified Application Integration and Testing
CIO	Chief Information Office
CJA	Critical Joint Applications
CLADRA	Classified Legacy Applications Deployment Readiness Activity
CLIN	Contract Line Item Number
CNNOC	Commander, Naval Network Operations Command
CNNWC	Command Navy Network Warfare Command
CNO	Chief of Naval Operations
CO	Commanding Officer
COR	Contract Officer's Representative
COTS	Commercial Off the Shelf
CPIAB	Classified PoP-In-A-Box
CPM	Customer Project Manager
CRFS	Classified Request For Service
CTR	Customer Technical Representative
DAA	Designated Approval Authority
DADMS	DON Application and Database Management System
DAT	Development Approach Team
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DMT	Data Management Team
DNS	Domain Name System
DoD	Department of Defense
DON	Department of the Navy
DSL	Definitive Software Library
EAGLE	Enterprise Application Group for Legacy and Emerging
EQRC	Enterprise Quarantine Reduction Coordinator
ERQ	Engineering Review Questionnaires
ESO	Enterprise Solution Office

FAM	Functional Area Manager
FDA	Functional Data Administrator
FOUO	For Official Use Only
FTP	File Transfer Protocol
GOTS	Government Off the Shelf
GPO	Group Policy Object
HVAC	Heating, Ventilation, Air Conditioning
IA	Information Assurance
IATO	Interim Authority To Operate
IATC	Interim Authority to Connect
IATT	Information Assurance Tiger Team
IQRPL	IATT Quarantine Remediation Priority List
ISF	Information Strike Force
ISFTDB	ISF Tools Database
IT/IM	Information Technology/Information Management
IT-21	Information Technology for the 21st Century
LADRA	Legacy Application Deployment Readiness Activity
LAPOC	Legacy Application Point of Contact
LAQRG	Legacy Application Quarantine Remediation Guide
LATF	Legacy Application Task Force
LATG	Legacy Applications Transition Guide
LDSD&T	Local Deployment Solution Development and Testing
MCTN	Marine Corps Tactical Network
MSI	Microsoft Installer
NADTF	Navy Applications Database Task Force
NAT	Network Address Translation
Navy IO	Navy Information Officer
NCARP	NMCI Connection Approval Review Panel
NEADG	Navy Enterprise Application Development Guide
NETWARCOM	Naval Network Warfare Command
NMCEPP	Navy Marine Corps Enclave Protection Policy
NMCI	Navy Marine Corps Intranet
NOC	Network Operations Center
NOIS	NMCI Ordering Interface System
OCONUS	Outside Continental United States
PDA	Product Delivery Analyst, Personal Digital Assistant
PDM	Product Delivery Manager
PEO-IT	Program Executive Office for Information Technology
PIAB	Pop-In-A-Box

PIAN	Pop-in-a-NOC
PM	Program Manager
PMO	Program Management Office
POA&M	Plan of Action and Milestones
POC	Point of Contact
POR	Program of Record
QRG	Quarantine Remediation Group
QRP	Quarantine Reduction Process
RFS	Request for Service
RMERQ	Risk Mitigation Engineering Review Questionnaire
S&T	Science and Technology
SIL	Site Integration Lead
SM	Site Manager
SME	Subject Matter Expert
SMO	Stem Management Office
SPAWAR	Space and Naval Warfare Systems Command
SSAA	Systems Security Authorization Agreement
SSE	Site Solutions Engineering
STEM	Site Transition Execution Manager
TFWeb	Task Force Web
TST	Technical Solutions Team
URL	Uniform Resource Locator
UTAM	User-to-Application-Mapping
VPN	Virtual Private Network
WIT	Waiver Input Template